中國科學院數學研究所專刊

甲種　　第1號

堆壘素數論

華　羅　庚

中國科學院數學研究所編輯

中國科學院出版

1953 北京

中國科學院數學研究所專刊
甲種　　第1號

堆壘素數論

著　者	華　羅　庚
出版者	中國科學院
印刷者	上海藝文書局鑄字印刷廠
經售者	中國圖書發行公司

書號 53015（數）02　　1953年6月初版
（滬）0001—3,000　　定價：白報紙本 ~~20,000~~ 元
道林紙本 35,000 元

中國科學院數學研究所專刊

甲種　　　第1號

堆壘素數論

華　羅　庚

中國科學院數學研究所編輯

中國科學院出版

1953 北京

謹以此書祝中蘇邦交永篤

華羅庚
1941年2月18日

В ЗНАК ВЕЧНОЙ ДРУЖБЫ
МЕЖДУ
КИТАЕМ И СССР
С ГЛУБОКИМ УВАЖЕНИЕМ

АВТОР

序

這一本小書能夠用本國文字出版是和人民民主政權分不開的．回憶一下離初稿完成的日子已經過了十二個年頭了，離俄文版刊出的日子也已隔了六年了．在解放以前漫長的歲月中，這書在我國刊出的問題，由即將出版、等待出版一直演變到把原稿搞得無影無蹤，以致於到了今天，在中國科學院敦促之下我還得從俄文本翻譯出來付印．這些事實，有力地說明了，舊政權是怎樣腐化怎樣地不關心科學，而人民民主政權又是怎樣地寶愛科學成果．

十二個年頭不算短暫，科學工作又有了不少的進展，所以僅把俄文本翻譯付印，是不合當前的情况的．我改寫了幾章，特別是第五章我把維諾格拉陀夫院士在 1942 到 1947 年進一步的創造性的工作及著者 1947 的工作包括進去．

在工作完成的時候，心情是異常愉快的．不但由於我的小書得以在祖國出版，而特別是從前所渴望着的中蘇兩國的友誼今天是實現了——已經牢不可破了！沒有中國科學院的鼓勵，這本書是不可能再出版的，所以我由衷地表示感謝．數學研究所的同人分頭負責核閱及訂正，人數之多使我不能在這兒一一列舉．祇有在集體主義的今天才會出現這樣的友愛團結的精神．而這又證明了人民民主政權的優越性．

華羅庚

北京，1953 年 5 月

俄文版原序*

本文中敍述了關於堆壘素數論的新結果，這一學科的基礎是由 И. М. 維諾格拉陀夫院士所奠立的，而由著者發展的．在第五、六兩章把開拓了新途徑的維諾格拉陀夫院士的工作加以簡化與改變而重述出來．閱讀本文，除了定理 7·14 之外，並不要求有任何其他較專門化的知識．

本文中大部份是著者所獲得並在這裏首次發表的結果的系統敍述．

無論著者如何地感謝維諾格拉陀夫院士都不會是過份的．

閔嗣鶴、鍾開萊兩位先生對於本文手稿之準備都曾給予幫助．

最後，著者對蘇聯科學院對他的著作的好評價願表示深切的謝意．在這些困難的日子裏，我們的科學研究的成果能獲得最友好的人民的最高權威方面的贊助，這特別給予我們很大的鼓舞．這種文化的合作是永遠寶貴的，而在現在的時刻，這更具有特殊的意義．謹祝此書的出版將會加強我們兩偉大人民間的眞誠友誼與相互親善．

華 羅 庚
中國昆明國立清華大學
1941 年 2 月 18 日

在幾年的戰爭之後，承維諾格拉陀夫院士給予我訪問蘇聯的機會．我非常高興地獲悉我在 1940--1941 年所寫的這篇論文已在印付．在 1942 年維諾格拉陀夫院士已把他的方法更精密化，而著者在到莫斯科之前還完全不知道．他的精密化加強了關於平均值的定理(本文中的定理 7)．藉助這一定理我們可以改進定理 8, 9, 11, 13, 17 等等．例如定理 11 對於 $s \geqslant 10\, k^2 \log k$ 也眞實，而定理 13 對於 $s \geqslant s_0 \sim 4\, k \log k$ 也正確，等等．

最後，我謹向翻譯此文的 Б. И. Сегал 與 Д. А. Басильков 兩位教授致謝．

華 羅 庚
莫斯科，1946 年 4 月 17 日

---

* 編者(指斯切克洛夫數學研究所專刊的編者)識：本書於 1941 年交數學研究所專刊編輯部，但由於 1941—1945 年的戰時條件，現在纔能出版．

說　明

本文並無一般的引言．各章的第一段有主要結果的敍述．本文中常引用下列符號：

對於實數 z，$[z]$ 表示不大於 z 的最大整數，而 $\{z\}$ 表示由 z 到最近整數的距離．

$e(z)=e^{2\pi iz}$．　　$e_q(x)=e^{2\pi ix/q}$．

k 表示一正整數；P 是充分大的正數，而 $L=\log P$．

$\max(a,b,\cdots,g)$ 表示 $a,b,\cdots,g$ 中最大的一個，而 $\min(a,b,\cdots,g)$ 表示其中最小的一個．

如習常所用：$a\mid b$ 表示 a 整除 b，$a\nmid b$ 表示 a 不整除 b．本文中常用 p 表示素數，$p^l\parallel n$ 表示 $p^l\mid n$ 而 $p^{l+1}\nmid n$．

$c(a,b,\cdots,g)$ 表示某一依存於 $a,b,\cdots,g$ 的正數；ε 是任意小正數，但不一定在每次出現時都是一樣的．

$f(x)=O(\varphi(x))$ 或 $f(x)\ll\varphi(x)$ 表示

$$|f(x)|\leqslant c(a,b,\cdots,g)\,\varphi(x).$$

在陳述定理時我們不用符號 $\ll$ 及 O，而用如以上形式的不等式．在證明中或引理中如果用到符號 $\ll$ 或 O，則其所包有的常數僅依賴於定理敍述中所涉及的 $a,b,\cdots,g$．

如有特別聲明，符號的含義可能有局部性的改變．

內　容

第　一　章

三　角　和

§1. 定理及基本引理的叙述

定理 1. 命 $f(x)$ 代表一個有整數係數的多項式

$$f(x) = a_k x^k + \cdots + a_1 x + a_0.$$

若 $(a_k, \cdots, a_1, q) = 1$，則

$$\left| \sum_{x=1}^{q} e^{2\pi i f(x)/q} \right| \leqslant c_1(k, \varepsilon)\, q^{1-\frac{1}{k}+\varepsilon},$$

此處 ε 是一任與的正數.

為了簡單起見,我們引用下面的符號:

$$a = \frac{1}{k}, \quad e_q(x) = e^{2\pi i x/q}$$

及

$$S(q, f(x)) = \sum_{x=1}^{q} e_q(f(x)).$$

基本引理 (**引理 1·1**). 若 $p \nmid (a_k, \cdots, a_1)$，則

$$|S(p^l, f(x))| \leqslant c_2(k)\, p^{l(1-a)}.$$

§2. 由基本引理推出定理

引理 1·2. 用 $\nu(q)$ 表示 q 的不同的素數因子的個數. 用 $d(q)$ 表 q 的正除數的個數. 則

$$2^{\nu(q)} \leqslant d(q) \leqslant c_3(\varepsilon)\, q^{\varepsilon}.$$

證：若素數 $p > 2^{1/\varepsilon}$，則

$$\frac{d(p^l)}{p^{l\varepsilon}} = \frac{l+1}{p^{l\varepsilon}} \leqslant \frac{l+1}{2^l} = \frac{l+1}{(1+1)^l} \leqslant \frac{l+1}{l+1} = 1 .$$

又若素數 $p \leqslant 2^{1/\varepsilon}$ 及 $l \geqslant 1$，則

$$\frac{d(p^l)}{p^{l\varepsilon}} = \frac{l+1}{p^{l\varepsilon}} \leqslant \frac{l+1}{2^{l\varepsilon}} \leqslant \frac{l+1}{l\varepsilon \log 2} \leqslant \frac{2}{\varepsilon \log 2} .$$

命 $q = p_1^{l_1} \cdots p_s^{l_s}$，此處 $p_1, \cdots, p_s$ 是 q 所有的不同的素因子，則

$$\frac{d(q)}{q^\varepsilon} = \prod_{p|q} \frac{d(p^l)}{p^{l\varepsilon}} \leqslant \prod_{p \leqslant 2^{1/\varepsilon}} \frac{2}{\varepsilon \log 2} = c_3(\varepsilon) .$$

引理中第一不等式顯然眞實.

引 理 1·3. 若 $(q_1, q_2) = 1$ 及 $f(0) = 0$，則

$$S(q_1 q_2, f(x)) = S(q_1, f(q_2 x)/q_2)\ S(q_2, f(q_1 x)/q_1) .$$

證：命 $x = q_1 y + q_2 z$. 當 y 及 z 各經過以 q_2 及 q_1 爲模的完全剩餘系，則 x 經過以 $q_1 q_2$ 爲模的完全剩餘系. 顯然得出

$$e_{q_1 q_2}(f(q_1 y + q_2 z)) = e_{q_2}(f(q_1 y)/q_1)\, e_{q_1}(f(q_2 z)/q_2) ,$$

及

$$\begin{aligned} S(q_1 q_2, f(x)) &= \sum_{x=1}^{q_1 q_2} e_{q_1 q_2}(f(x)) = \\ &= \sum_{y=1}^{q_2} \sum_{z=1}^{q_1} e_{q_2}(f(q_1 y)/q_1)\ e_{q_1}(f(q_2 z)/q_2) = \\ &= S(q_1, f(q_2 x)/q_2)\ S(q_2, f(q_1 x)/q_1) . \end{aligned}$$

定理的證明. 我們可以假定 $a_0 = 0$ 而不失其普遍性. 命 $q = p_1^{l_1} \cdots p_s^{l_s}$，此處 $p_1, \cdots, p_s$ 是 q 所有的不同的素因子. 由引理 1·3

$$S(q, f(x)) = \prod_{p|q} S\left(p^l, \frac{f(q\, x/p^l)}{q/p^l}\right),$$

及由引理 1·1 可得

$$\left| S(q, f(x)) \right| \leqslant c_2^{\nu(q)} q^{1-\epsilon}.$$

再由引理 1·2（我們可設 $c_2 > 1$），

$$c_2^{\nu(q)} = (2^{\nu(q)})^{\log c_2/\log 2} \leqslant c_1(k, \varepsilon) q^{\varepsilon}.$$

由此卽得出本定理.

§3. 當 $l=1$ 時基本引理的證明(Mordell*)

並不失去普遍性,我們可以假定 $p > k$ 及 $a_0 = 0$. 爲了簡單起見,我們用 $\sum\limits_{x}$ 代表 $\sum\limits_{x=1}^{p}$. 如是得到

$$\sum_{a_k} \cdots \sum_{a_1} \left| \sum_{x} e_p(a_k x^k + \cdots + a_1 x) \right|^{2k} =$$

$$= \sum_{x_1} \cdots \sum_{x_k} \sum_{y_1} \cdots \sum_{y_k} \sum_{a_k} \cdots \sum_{a_1} e_p(a_k(x_1^k + \cdots + x_k^k - y_1^k - \cdots - y_k^k) +$$

$$+ \cdots + a_1(x_1 + \cdots + x_k - y_1 - \cdots - y_k)) = p^k N,$$

此處 N 表示下列相合式組的解答的個數:

$$x_1^h + \cdots + x_k^h \equiv y_1^h + \cdots + y_k^h \pmod p, \quad 1 \leqslant h \leqslant k, \quad 1 \leqslant x, y \leqslant p. \qquad (1)$$

注意,獲得此結論時,引用了下面的公式

$$\sum_{x=1}^{q} e_q(hx) = \begin{cases} q & 若\ q \mid h, \\ 0 & 若\ q \nmid h. \end{cases}$$

由對稱函數中一習知的定理,由 (1) 可以引出

* *Quarterly Jour. of Math.*, **3** (1932), 161–167.

$$(x-x_1)\cdots(x-x_k)\equiv(x-y_1)\cdots(x-y_k)\pmod p.$$

由此可知 $y_1,\cdots,y_k$ 乃由 $x_1,\cdots,x_k$ 轉換次序而得出的 (mod p). 所以

$$N\leqslant k!\,p^k.$$

由此得出

$$\sum_{a_k}\cdots\sum_{a_1}\left|S(p,a_kx^k+\cdots+a_1x)\right|^{2k}\leqslant k!\,p^{2k}. \tag{2}$$

顯然,對任一 $\lambda\,(\not\equiv 0\pmod p)$ 及 任一 μ 常有

$$|S(p,f(x))|=|S(p,f(\lambda x+\mu)-f(\mu))|.$$

所有這種形式的和都在 (2) 式的左邊出現. 今往求出由所有不同的多項式 $f(\lambda x+\mu)-f(\mu)$ 所得的和 $S(p,f(\lambda x+\mu)-f(\mu))$ 的個數. 若二多項式的係數各各相合 (mod p), 則此二多項式算爲全同, mod p. 我們可以假定 $p\nmid a_k$ 而不失其普遍性. 若 $f(\lambda x+\mu)-f(\mu)$ 與 $f(x)$ 全同, mod p, 則得

$$a_k\lambda^k\equiv a_k,\qquad k\,a_k\lambda^{k-1}\mu+a_{k-1}\lambda^{k-1}\equiv a_{k-1}\pmod p.$$

適合 $\lambda^k\equiv 1\pmod p$ 的 λ 的個數 $\leqslant k$. 對一固定的 λ, μ 就唯一決定. 所以形如 $f(\lambda x+\mu)-f(\mu)$ 的多項式中最多有 k 個與 $f(x)$ 全同, mod p.

由此可得,在所有的 $p(p-1)$ 個多項式

$$f(\lambda x+\mu)-f(\mu),\qquad 1\leqslant\lambda\leqslant p-1,\qquad 1\leqslant\mu\leqslant p,$$

中,至少有 $p(p-1)/k$ 個是和 $f(x)$ 相同的. 所以

$$a\,p\,(p-1)\,|S(p,f(x))|^{2k}\leqslant k!\,p^{2k},$$

即

$$|S(p,f(x))|\leqslant\left(\frac{k\cdot k!}{p\,(p-1)}\right)^{\frac{1}{2}a}p\leqslant(2k\cdot k!)^{\frac{1}{2}a}p^{1-a}. \tag{3}$$

§4. 幾 條 引 理

引 理 1·4. 假定 $s(x)$ 是一整數係數的多項式, mod p. a 是 $s(x)\equiv 0$

(mod p) 的 m 重根. $p^u \| s(px+\alpha)$*. 命 $t(x)=p^{-u}s(px+\alpha)$, 則相合式

$$t(x)\equiv 0 \pmod p$$

至多有 m 個根.

證: 並不失其普遍性,可以假定 $\alpha=0$. 如此則

$$s(x)=x^m s_1(x)+p s_2(x),$$

此處 $s_1(0)\not\equiv 0 \pmod p$, $s_2(x)$ 的次數低於 m. $s_1(x)$ 及 $s_2(x)$ 都是整係數多項式. 由此得出

$$s(px)=p^m x^m s_1(px)+p s_2(px).$$

因爲 x^m 的係數 $p^m s_1(0)$ 不能爲 p^{m+1} 所整除, 所以 $u\leqslant m$. 又因爲 $p^{-u}s(px)$ 的次數 $\leqslant m \pmod p$, 所以證明了本引理.

引 理 1·5. 假定

$$f(x)=a_k x^k+\cdots+a_1 x,$$

$p\nmid(a_k,\cdots,a_1)$ 及 $p^t\|(ka_k,\cdots,2a_2,a_1)$. 又假定 μ 是相合式

$$f'(x)\equiv 0 \pmod{p^{t+1}},\qquad 0\leqslant x<p,$$

的根. 如果 p^σ 恰能整除 $f(\mu+py)-f(\mu)$ 所有的係數,則

$$1\leqslant\sigma\leqslant k.$$

證: 假定 $\sigma\geqslant k+1$, 則由於 p^σ 能整除 $f(\mu+py)-f(\mu)$ 所有的係數,可知

$$p^\sigma \left| \frac{p^h}{h!} f^{(h)}(\mu),\right.\qquad 0\leqslant h\leqslant k.$$

* $p^u \| g(x)$ 表示 p^u 整除 $g(x)$ 的所有的係數,但 p^{u+1} 不能.

卽對任一 h 常有

$$p^{k+1} \mid \frac{p^h}{h!} f^{(h)}(\mu),$$

由此得出

$$p \left| \frac{1}{h!} f^{(h)}(\mu) \right. .$$

因而得出 $p \mid a_k$, $p \mid a_{k-1}, \cdots, p \mid a_1$. 此與假定 $p \nmid (a_k, \cdots, a_1)$ 相違背.

§5. 基本引理的證明

基本引理可以由以下的更明確的引理來概括.

引理 1·6. 命 $f(x) = a_k x^k + \cdots + a_1 x + a_0$. $p \nmid (a_k, \cdots, a_1)$. 則

$$|S(p^l, f(x))| \leqslant k^3 p^{(1-a)l}.$$

證: 命 t 是能整除 $(ka_k, \cdots, 2a_2, a_1)$ 的 p 的最高方次. 又設 $\mu_1, \cdots, \mu_r$ 是相合式

$$f'(x) \equiv 0 \pmod{p^{t+1}}, \qquad 0 \leqslant x < p,$$

的相異的根. 其重數分別爲 $m_1, \cdots, m_r$. 命 $m_1 + \cdots + m_r = m$, 易見 $m \leqslant k-1$. 此引理顯然是不等式

$$|S(p^l, f(x))| \leqslant k^2 \max(1, m) p^{(1-a)l}$$

的直接推理. 而此式又顯然是 §3 的 (3) 式及以下定理的直接推理: 若 $l > 1$, 則

$$|S(p^l, f(x))| \leqslant k^2 m p^{(1-a)l}. \tag{4}$$

現在用數學歸納法來證明上式.

由於 $p \nmid (a_k, \cdots, a_1)$ 及 $p^t \| (ka_k, \cdots, 2a_2, a_1)$, 所以一定有 $p^t \leqslant k$.

1) 假定 $l < 2(t+1)$. 如果 $t = 0$, 則得 $l = 1$. 這是已經討論過的情況. 若 $t \geqslant 1$, 則顯然可見

$$|S(p^l, f(x))| \leqslant p^l \leqslant p^{l(1-a)} \cdot p^{(2t+1)a} \leqslant p^{l(1-a)} k^{(2+1/t)a} \leqslant k^2 p^{l(1-a)},$$

故引理成立.

2) 假定 $l \geqslant 2(t+1)$. 寫

$$S(p^l, f(x)) = \sum_{\nu=1}^{p} \sum_{\substack{0 \leqslant x \leqslant p^l - 1 \\ x \equiv \nu \pmod p}} e_{p^l}(f(x)) = \sum_{\nu=1}^{p} S_\nu .$$

如果 ν 並非 μ_i 之一,則命

$$x = y + p^{l-t-1} z, \quad 0 \leqslant y < p^{l-t-1}, \quad 0 \leqslant z < p^{t+1},$$

卽得

$$S_\nu = \sum_{\substack{0 \leqslant x < p^l \\ x \equiv \nu \pmod p}} e_{p^l}(f(x) = \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv \nu \pmod p}} \sum_{0 \leqslant z < p^{t+1}} e_{p^l}(f(y) + p^{l-t-1} z f'(y)) =$$

$$= \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv \nu \pmod p}} e_{p^l}(f(y)) \sum_{z=0}^{p^{t+1}} e_{p^{t+1}}(z f'(y)) = 0, \tag{5}$$

最後等式是由於 $f'(y) \not\equiv 0 \pmod{p^{t+1}}$.

如果 $\nu = \mu_i$, 則依引理 1·5 來定義 σ_i, 如此則得

$$S_{\mu_i} = \sum_{\substack{x=1 \\ x \equiv \mu_i \pmod p}}^{p^l} e_{p^l}(f(x)) = \sum_{y=1}^{p^{l-1}} e_{p^l}(f(\mu_i + p y)) =$$

$$= e_{p^l}(f(\mu_i)) \sum_{y=1}^{p^{l-1}} e_{p^{l-\sigma_i}}(p^{-\sigma_i}(f(\mu_i + p y) - f(\mu_i))).$$

命 $g_i(x) = p^{-\sigma_i}(f(\mu_i + p y) - f(\mu_i))$. 由引理 1·5 可知

$$|S_{\mu_i}| = p^{\sigma_i - 1} |S(p^{l-\sigma_i}, g_i(x))| \leqslant$$

$$\leqslant p^{\sigma_i(1-\alpha)} |S(p^{l-\sigma_i}, g_i(x))|.$$

總括 (5), (6) 二式得出

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i(1-a)} |S(p^{l-\sigma_i}, g_i(x))|. \tag{6}$$

如果 $l \geqslant \max(\sigma_1, \cdots, \sigma_r)$,則用歸納法並引理 1·4, 由 (6) 式可得

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} m_i p^{\sigma_i(1-a)} k^2 p^{(l-\sigma_i)(1-a)} < mk^2 p^{l(1-a)}.$$

若 $l < \max(\sigma_1, \cdots, \sigma_r)$, 則 $l \leqslant k$

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i-1} p^{l-\sigma_i} \leqslant k p^{l(1-a)}.$$

由是基本引理即已完全證明.

所以定理 1 也就已經完全證明.

§6. 推 論

在論述若干推理之前,我們先引入關於整值多項式的觀念.

定 義. 如果對整數 x, 一多項式 $f(x)$ 的值也是整數, 這多項式就稱爲整值多項式.

引 理 1·7. 命

$$v! F_v(x) = x(x-1)\cdots(x-v+1).$$

一多項式是整值多項式的必要且充分條件是它可以表成

$$a_k F_k(x) + \cdots + a_1 F_1(x) + a_0$$

的形式,此處 $a_k, \cdots, a_1, a_0$ 都是整數.

證: 顯然 $F_v(x)$ 是整值多項式, 所以 $a_k F_k(x) + \cdots + a_1 F_1(x) + a_0$ 也是整值多項式.

反之,任一多項式常可表成

$$f(x) = b_k F_k(x) + \cdots + b_1 F_1(x) + b_0.$$

連續以 $x=0, 1, 2, \cdots, k$ 代入上式,可知諸 b 一定是整數.

現在可敘述本章的定理及基本引理的推論.

推論 1·1. 命 $f(x)$ 是一 k 次整值多項式，它的係數的最小公分母用 d 表示. 設 $p^t \| d$, 並且假定並非 $f(x)$ 的所有的非常數項的係數都是 p 的倍數. 則

$$\left| \sum_{x=1}^{p^{l+t}} e_{p^l}(f(x)) \right| \leqslant c_4(k)\, p^{l(1-a)}.$$

證: 由於 $d \mid k!$，所以得此推論.

推論 1·2. 命 $f(x)$ 是一 k 次整值多項式，它的係數的最小公分母是d. 假定並無素數 p 使相合式

$$f(x) \equiv f(0) \pmod p$$

對所有的 x 皆能成立. 則

$$\left| \sum_{x=1}^{\bar{q}} e_q(f(x)) \right| \leqslant c_5(k, \varepsilon)\, q^{1-a+\varepsilon},$$

此處 $\bar{q} = q \cdot (d, q)$.

推論 1·3. 仍如推論 1·1 及 1·2 的假定,我們有

$$\left| \sum_{\substack{x=1 \\ p \nmid x}}^{p^{l+t}} e_{p^l}(f(x)) \right| \leqslant c_6(k)\, p^{(1-a)l}$$

及

$$\left| \sum_{\substack{x=1 \\ (x,q)=1}}^{\bar{q}} e_q(f(x)) \right| \leqslant c_7(k, \varepsilon)\, q^{1-a+\varepsilon}.$$

證: 我們現在僅證明第一不等式,第二式可由第一式推得. 顯然有

$$\sum_{\substack{x=1 \\ p \nmid x}}^{p^{l+t}} e_{p^l}(f(x)) = \sum_{x=1}^{p^{l+t}} e_{p^l}(f(x)) - \sum_{x=1}^{p^{l+t-1}} e_{p^l}(f(px)).$$

寫

$$df(x) = a_k x^k + \cdots + a_1 x + a_0, \quad p \nmid (a_k, \cdots, a_1).$$

命 p^{μ} 是 p 的最高方次可以整除 $(f(px)-f(0))\,d$ 的所有的係數者. 顯然 $\mu\leqslant k$. 所以當 $l\geqslant\mu$ 時,

$$\left|\sum_{x=1}^{p^{l+t-1}} e_{p^l}(f(px))\right| = \left|\sum_{x=1}^{p^{l+t-1}} e_{p^{l+t-\mu}}(f(px)\cdot p^{t-\mu})\right| \leqslant$$
$$\leqslant p^{\mu-1}\cdot c_4(k)\,p^{(l-\mu)(1-a)} \leqslant$$
$$\leqslant c_4(k)\,p^{l(1-a)-1+\mu a} \leqslant c_4(k)\,p^{l(1-a)}.$$

若 $l<\mu\leqslant k$, 則顯然有

$$\left|\sum_{x=1}^{p^{l+t-1}} e_{p^l}(f(px))\right| \leqslant p^{l+t-1} \leqslant k!\,p^{l-1} \leqslant k!\,p^{(1-a)l}.$$

§7. 有限的富利埃級數

引理 1·8. 命

$$S=\sum_{q'<n\leqslant q''} e(n\alpha), \qquad e(x)=e^{2\pi ix}.$$

則得

$$|S|\leqslant\min\left(q''-q', \frac{1}{2\{\alpha\}}\right),$$

此處 $\{\alpha\}$ 代表從 α 到和它最接近的整數的距離. 換言之, $\{\alpha\}=\min(\alpha-[\alpha], [\alpha]+1-\alpha)$.

證: 顯然有不等式 $|S|\leqslant q''-q'$. 若 $\alpha\neq[\alpha]$, 命 $Q=q''-q'$, 則有

$$\left|\sum_{q'<n\leqslant q''} e(n\alpha)\right| = \left|\sum_{n=0}^{Q-1} e(n\alpha)\right| = \left|\frac{1-e(Q\alpha)}{1-e(\alpha)}\right| \leqslant \frac{2}{|1-e(\alpha)|} =$$
$$=\frac{1}{|\sin\pi\alpha|}\leqslant\frac{1}{2\{\alpha\}}.$$

(當 $0\leqslant\xi\leqslant\frac{1}{2}$ 時 $\sin\pi\xi>2\xi$, 所以有 $|\sin\pi\xi|\geqslant2\{\xi\}$).

引理 1·9. 命 $g(x)$ 表一週期是 q 的函數, 且

$$g(x)=\begin{cases}1 & \text{當 } 0<x<m,\\ 0 & \text{當 } m\leqslant x<q.\end{cases}$$

則

$$g(x)=\frac{m}{q}+\sum_{n=1}^{q-1} e_q(nx)\frac{1-e_q(-nm)}{1-e_q(-n)}.$$

證：顯然 $g(x)$ 可以表成

$$g(x)=\frac{1}{q}\sum_{n=0}^{q-1} e_q(nx)\sum_{t=0}^{m-1} e_q(-nt)=$$

$$=\frac{m}{q}+\frac{1}{q}\sum_{n=1}^{q-1} e_q(nx)\frac{1-e_q(-nm)}{1-e_q(-n)}.$$

§8.

定理 2. 設 $f(x)=a_k x^k+\cdots+a_1 x+a_0$ 是一整數係數多項式．命 $(a_k,\cdots,a_2,q)=d$，則

$$\left|\sum_{x=1}^{m} e_q(f(x))-\frac{m}{q}S(q,f(x))\right|\leqslant c_8(k,\varepsilon)\,q^{1-a+\varepsilon}d^a.$$

又當 $1\leqslant m\leqslant q$ 時

$$\left|\sum_{x=1}^{m} e_q(f(x))\right|\leqslant c_9(k,\varepsilon)\,q^{1-a+\varepsilon}d^a.$$

證：由引理 1·9 已知

$$\sum_{x=1}^{m} e_q(f(x))=\sum_{x=1}^{q} e_q(f(x))\,g(x)=$$

$$=\frac{m}{q}\cdot S(q,f(x))+\frac{1}{q}\sum_{x=1}^{q} e_q(f(x))\sum_{n=1}^{q-1} e_q(nx)\frac{1-e_q(-nm)}{1-e_q(-n)}.$$

卽得（由引理 1·8）

$$\left|\sum_{x=1}^{m} e_q(f(x))-\frac{m}{q}S(q,f(x))\right|\leqslant\frac{1}{q}\sum_{n=1}^{q-1}\frac{1}{2\left\{\frac{n}{q}\right\}}\left|\sum_{x=1}^{q} e_q(f(x)+nx)\right|\leqslant$$

$$\leqslant\sum_{n=1}^{q}\frac{1}{n}\left|\sum_{x=1}^{q} e_q(f(x)+nx)\right|.$$

命 $(d, a_1+n)=q'$，則由定理 1 可知

$$\sum_{n=1}^{q}\frac{1}{n}\left|\sum_{x=1}^{q}e_q(f(x)+nx)\right| \leqslant \sum_{q'|d}\sum_{\substack{n=1\\ a_1+n\equiv 0 \pmod{q'}}}^{q}\frac{1}{n}\left|\sum_{x=1}^{q}e_{q/q'}\left(\frac{f(x)+nx}{q'}\right)\right| \ll$$

$$\ll \sum_{q'|d}\sum_{\substack{n=1\\ a_1+n\equiv 0 \pmod{q'}}}^{q}\frac{1}{n}\, q'(q/q')^{1-a+\epsilon} \ll$$

$$\ll q^{1-a+\epsilon}\sum_{q'|d}q'^{a}\sum_{\substack{n=1\\ a_1+n\equiv 0 \pmod{q'}}}^{q}\frac{1}{n} \ll$$

$$\ll q^{1-a+\epsilon}\left(\sum_{q'|d}q'^{a}\sum_{l=1}^{q/q'}\frac{1}{q'l}+\sum_{q'|d}q'^{a}\right) \ll$$

$$\ll q^{1-a+\epsilon}\sum_{q'|d}q'^{a} < q^{1-a+\epsilon}d^{\epsilon}.$$

第 二 章

包含除數函數的和的估值

§1. 引　　言

本章的目的在證明以下的定理.

定理 3. 命 $f(x_1, x_2, \cdots, x_n)$ 代表一個 k 次多項式,它的係數是整數,並假定所有的係數的最大公約數是 1, 則

$$\sum_{\substack{x_1=1 \\ f(x_1,\cdots,x_n)\neq 0}}^{P} \cdots \sum_{x_n=1}^{P} d^l(|f(x_1,\cdots,x_n)|) \leqslant c_1(k,n,l)\, A\, (\log X)^{c_2(k,n,l)},$$

此處 X 表 $|f(x_1, \cdots, x_n)|$ 在 $1 \leqslant x_1, \cdots, x_n \leqslant P$ 中的最大值, $A = \max(P^n, X^{n/k})$.

注意, 此處 c_1 及 c_2 與 $f(x_1, \cdots, x_n)$ 的係數並無關係. 由此定理容易引出下面較廣泛的推理:

命 $f(x_1, \cdots, x_n)$ 代表一個 k 次整係數多項式. 命 m 代表它的所有的係數的最大公約數,則

$$\sum_{\substack{x_1=1 \\ f(x_1,\cdots,x_n)\neq 0}}^{P} \cdots \sum_{x_n=1}^{P} d^l(|f(x_1,\cdots,x_n)|) \leqslant c_1(k,n,l)\, A\, (\log X)^{c_2(k,n,l)}\, d^l(m).$$

定理 3 的證明依賴於 van der Corput 的一個引理 (§ 2) 和第一章所證明的關於三角和的結果.

§ 2. van der Corput 的引理*

引理 2·1. 設有正數 A 及 γ 存在,使

* *Proc. Akad. Wetensch. Amsterdam,* **42** (1939).

$$\sum_{\substack{y=1 \\ v|y}}^{X} T(y) \leqslant A \prod_{\sigma=1}^{s} \frac{x(p_\sigma, \alpha_\sigma)}{p_\sigma}, \qquad v = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \leqslant X^\gamma,$$

此處 $x(p_\sigma, \alpha_\sigma) \geqslant 0$; 且

$$\sum_{\alpha=1}^{\infty} (\alpha+1)^{(1+2/\gamma)l} x(p, \alpha) \leqslant C,$$

此處 C 與素數 p 無關. 又當 $v=1$, $s=0$ 時,有不等式

$$\sum_{y=1}^{X} T(y) \leqslant A.$$

則

$$S = \sum_{y=1}^{X} d^l(y)\, T(y) \leqslant c_3(l, C, \gamma)\, A\, (\log X)^C.$$

證: 把 y 寫成 $y = P_1 P_2 \cdots P_m w$, 此處 P 經過 y 的所有大於 X^γ的素數因子. 以 v_1 表 w 的不大於 X^γ 之最大因子, v_2 表 w/v_1 的不大於 X^γ之最大因子,依此進行. 假定此手續止於 n 次,則 y 可以表成

$$y = P_1 \cdots P_m v_1 \cdots v_n.$$

這 n 將稱為 y 的指標,而 $v_1, \cdots, v_n$ 將稱為 y 的特徵因數.

顯然有 $v_{n-1} \geqslant X^{\frac{1}{2}\gamma}$, 由此得

$$X^{\gamma m} \leqslant P_1 \cdots P_m \leqslant X, \quad X^{\frac{1}{2}(n-1)\gamma} \leqslant v_1 \cdots v_{n-1} \leqslant X,$$

即得

$$m \leqslant \frac{1}{\gamma}, \qquad n \leqslant 1 + \frac{2}{\gamma}.$$

由 $d(\lambda\mu) \leqslant d(\lambda)\, d(\mu)$, 可知

$$d(y) \leqslant 2^m d(v_1) \cdots d(v_n) \leqslant 2^{1/\gamma} d(v_1) \cdots d(v_n).$$

顯然有

$$d^l(y) \leqslant \begin{cases} 2^{l/\gamma} & 若\ n=0, \\ 2^{l/\gamma} \max\limits_{\nu} d^{ln}(v_\nu) \leqslant 2^{l/\gamma} \sum\limits_{\nu=1}^{n} d^{ln}(v_\nu) & 若\ n>0. \end{cases}$$

寫

$$S = \sum_{y=1}^{X} d^l(y)\, T(y) = \sum_{0 \leqslant n \leqslant 1+2/\gamma} U_n,$$

分和 U_n 代表 S 中所有 y 的指標是 n 的項之和.

當 $n=0$ 時,

$$U_0 \leqslant 2^{l/\gamma} \sum_{y=1}^{X} T(y) \leqslant 2^{l/\gamma} A.$$

若 $1 \leqslant n \leqslant 1+\dfrac{2}{\gamma}$, 則

$$U_n \leqslant 2^{l/\gamma} \sum_{\nu=1}^{n} U_{n\nu},$$

其中

$$U_{n\nu} = \sum_{y=1}^{X}{}' d^{ln}(v_\nu)\, T(y),$$

此處 $\sum\limits_{y=1}^{X}{}'$ 表示一個和,其中 y 經過一切指標是 n 的數,且以 v_ν 做它的第 ν 個特徵因子者. 已知 $2 \leqslant v_\nu \leqslant X^\gamma$, 所以

$$U_{n\nu} \leqslant \sum_{2 \leqslant v \leqslant X^\gamma} d^{ln}(v) \sum_{y=1}^{X}{}'' T(y),$$

此處 Σ'' 表示一個和, 其中 y 的指標是 n 且以 v_ν 做它的第 ν 個特徵因子者.
因此

$$\sum_{y=1}^{X}{}'' T(y) \leqslant \sum_{\substack{y=1 \\ v \mid y}}^{X} T(y) \leqslant A \prod_{\sigma=1}^{s} \frac{x(p_\sigma, a_\sigma)}{p_\sigma}.$$

由於 $d(\nu)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)$，可知

$$U_{n\nu}\leqslant A\sum_{2\leqslant\nu\leqslant X^Y}\prod_{\sigma=1}^{s}\frac{(\alpha_\sigma+1)^{ln}\chi(p_\sigma,\alpha_\sigma)}{p_\sigma}\leqslant$$

$$\leqslant A\prod_{p\leqslant X^Y}\left(1+\sum_{\alpha=1}^{\infty}\frac{(\alpha+1)^{ln}\chi(p,\alpha)}{p}\right)\leqslant$$

$$\leqslant A\,e^R\leqslant c_3'\,A\,e^{c\log\log X}\leqslant c_3'\,A\,(\log X)^C,$$

此處 $R=c\sum_{p\leqslant X^Y}\frac{1}{p}$. 代入關於 U_n 及 S 的不等式，由此即得出本引理.

（注意，在證明中用了等式

$$\sum_{p\leqslant X}\frac{1}{p}=\log\log X+O(1).$$

這是素數定理的推理. 當然也是引理 7·14 的推理.）

§3. 關於相合式解數的若干引理

引 理 2·2. 命 $f(x_1,\cdots,x_n)$ 是具有整數係數的 k 次多項式. 並且假定並非它所有的係數都是 p 的倍數. 則相合式

$$f(x_1,\cdots,x_n)\equiv 0 \pmod{p^a}$$

的解數 $\leqslant c_4(k,n)\,p^{na-1}$.

證：1) 當 $n=1$，這引理顯然正確，因爲相合式

$$f(x)\equiv 0 \pmod{p}$$

的根數不超過 k，所以原相合式的解數 $\leqslant k\,p^{a-1}$.

2) 將相合式 $f(x_1,\cdots,x_n)\equiv 0 \pmod{p^a}$ 寫成

$$f_s(x_1,\cdots,x_{n-1})\,x_n^s+\cdots+f_0(x_1,\cdots,x_{n-1})\equiv 0 \pmod{p^a}.$$

我們現用歸納法來證明本引理. 假定本引理對 $n-1$ 個變數是眞實的,則

$$f_s(x_1,\cdots,x_{n-1})\equiv 0 \pmod{p^\alpha}$$

的解數是 $O(p^{(n-1)\alpha-1})$. 如果 $f_s(x_1,\cdots,x_{n-1})\not\equiv 0 \pmod{p^\alpha}$, 則原式中 x_n 之值最多是 $O(p^{\alpha-1})$. 所以所討論的相合式的解數 $\leqslant c_4(k,n)\,p^{n\alpha-1}$.

引 理 2·3. 在引理 2·2 的假設下,相合式

$$f(x_1,\cdots,x_n)\equiv 0 \pmod{p^\alpha}$$

的解數 $\leqslant c_5(k,n)\,(\alpha+1)^{n-1}\,p^{n\alpha-\alpha a}$, 此處 $a={}^1/_k$.

證: 1) 當 $n=1$, 相合式

$$f(x)\equiv 0 \pmod{p^\alpha}$$

的解數等於

$$\frac{1}{p^\alpha}\sum_{h=1}^{p^\alpha}\sum_{x=1}^{p^\alpha}e_{p^\alpha}(h\,f(x)),\qquad e_q(x)=e^{2\pi ix/q}.$$

命

$$f(x)=a_k x^k+\cdots+a_1x+a_0.$$

若 $p|(a_k,\cdots,a_1)$ 而 $p\nmid a_0$, 則此相合式無解,引理顯然成立. 今假定 $p\nmid(a_k,\cdots,a_1)$. 由引理 1·1,

$$\left|\frac{1}{p^\alpha}\sum_{h=1}^{p^\alpha}\sum_{x=1}^{p^\alpha}e_{p^\alpha}(h\,f(x))\right|\leqslant\frac{1}{p^\alpha}\sum_{h=1}^{p^\alpha}\left|\sum_{x=1}^{p^\alpha}e_{p^\alpha}(h\,f(x))\right|=$$

$$=\frac{1}{p^\alpha}\sum_{\lambda=0}^{\alpha}\sum_{\substack{h=1\\ p^\lambda\| h}}^{p^\alpha}\left|\sum_{x=1}^{p^\alpha}e_{p^\alpha}(h\,f(x))\right|=O\left(\frac{1}{p^\alpha}\sum_{\lambda=0}^{\alpha}p^{\alpha-\lambda}\cdot p^\lambda\cdot p^{(\alpha-\lambda)(1-a)}\right)=$$

$$=O(p^{\alpha(1-a)}),$$

此處用上了

$$\sum_{\lambda=0}^{\alpha}p^{-\lambda(1-a)}=O(1).$$

2） 歸納法. 把式子

$$f(x_1, \cdots, x_n) \equiv 0 \pmod{p^\alpha}$$

寫成

$$g_k x_n^k + \cdots + g_0 \equiv 0 \pmod{p^\alpha}, \quad g_\nu = g_\nu(x_1, \cdots, x_{n-1}).$$

今分別討論使

$$p^\lambda \| (g_k, \cdots, g_0), \qquad \alpha > \lambda > 0, \tag{1}$$

以及使 $p^\alpha | (g_k, \cdots, g_0)$ 的整數組 $x_1, \cdots, x_{n-1}$. 在後一種情況之下，其解數是

$$O((\alpha+1)^{n-2} p^{(n-1)\alpha-a\alpha} p^\alpha) = O((\alpha+1)^{n-2} p^{n\alpha-a\alpha}).$$

今討論具有條件（1）的情況. 在所有的 g 之中，至少有一個並非所有的係數都是 p 的倍數的,以 g_μ 表之. 由歸納法假定,適合

$$g_\mu \equiv 0 \pmod{p^\lambda}, \qquad 0 \leqslant x_\nu < p^\alpha, \qquad 1 \leqslant \nu \leqslant n-1$$

的解數最多是

$$O((\alpha+1)^{n-2} p^{(n-1)(\alpha-\lambda)+(n-1)\lambda-\lambda a}) = O((\alpha+1)^{n-2} p^{(n-1)\alpha-\lambda a}),$$

即適合條件（1）的 $x_1, \cdots, x_{n-1}$ 的組數是 $O((\alpha+1)^{n-2} p^{(n-1)\alpha-\lambda a})$. 對每一組適合（1）的 $x_1, \cdots, x_{n-1}$，相合式

$$\frac{g_k}{p^\lambda} x_n^k + \cdots + \frac{g_0}{p^\lambda} \equiv 0 \pmod{p^{\alpha-\lambda}}, \quad 0 < x_n \leqslant p^\alpha,$$

最多有 $O(p^{\lambda+(\alpha-\lambda)(1-a)}) = O(p^{\alpha-(\alpha-\lambda)a})$ 個 x_n.

所以引理中所涉及的適合（1）的相合式的解是

$$O((\alpha+1)^{n-2} p^{(n-1)\alpha-\lambda a} p^{\alpha-(\alpha-\lambda)a}) = O((\alpha+1)^{n-2} p^{n\alpha-a\alpha}).$$

$\lambda = 0$ 時此結論也顯然眞實. 所以引理中相合式的個數是

$$O\left(\sum_{\lambda=0}^{\alpha} (\alpha+1)^{n-2} p^{n\alpha-a\alpha}\right) = O((\alpha+1)^{n-1} p^{n\alpha-a\alpha}).$$

§4. 定理的證明

在引理 2·1 中取 $T(y)$ 爲

$$|f(x_1,\cdots,x_n)| = y, \qquad 1 \leqslant x_\nu \leqslant P,$$

的解數. 則得

$$\sum_{\substack{x_1=1 \\ f(x_1,\cdots,x_n)\neq 0}}^{P} \cdots \sum_{x_n=1}^{P} d^l(|f(x_1,\cdots,x_n)|) = \sum_{y=1}^{X} d^l(y)\,T(y),$$

此處 X 是 $|f(x_1,\cdots,x_n)|$ 在 $1 \leqslant x_1,\cdots,x_n \leqslant P$ 中的極大值.

取 $\gamma = a$ 及

$$x(p,\alpha) = \begin{cases} O(1) \\ O((\alpha+1)^{n+1} p^{1-a\alpha}). \end{cases}$$

則

$$\sum_{y=1}^{X} T(y) = \sum_{x_1=1}^{P} \cdots \sum_{x_n=1}^{P} 1 = P^n = A,$$

而

$$\sum_{\substack{y=1 \\ p^\alpha | y}}^{X} T(y) \leqslant \left(\frac{P}{p^\alpha} + 1\right)^n M,$$

此處 M 是

$$f(x_1,\cdots,x_n) \equiv 0 \pmod{p^\alpha}$$

的解數. 由引理 2·2 及 2·3 可知

$$\sum_{\substack{y=1 \\ p^\alpha | y}}^{X} T(y) = O\left(A\left\{\begin{matrix} p^{-1} \\ (\alpha+1)^{n-1} p^{-a\alpha} \end{matrix}\right\}\right) = A\frac{x(p,\alpha)}{p}.$$

由於

$$\sum_{\alpha=1}^{\infty} (\alpha+1)^{(1+2/\gamma)l} x(p,\alpha) = O\left(\sum_{\alpha\leqslant k} (\alpha+1)^{(1+2k)l} + \right.$$

$$+\sum_{\alpha>k}(\alpha+1)^{(1+2k)l+n-1}p^{1-a\alpha}\Big)=O(1),$$

所以證明了我們的定理.

§ 5.

為了將來的應用,我們證明兩條較精密且特殊的結果，這些結果也是和除數函數和有關的.

引 理 2·4. 命 t 是一正整數,則

$$\sum_{0<z\leqslant P}\frac{(d(z))^t}{z}\leqslant c_6(t)(\log P)^{2^t}.$$

證: 當 $t=0$ 時上式顯然正確. 今設其對 $t-1$ 也真. 則

$$\sum_{0<z\leqslant P}\frac{(d(z))^t}{z}=\sum_{0<z\leqslant P}\frac{(d(z))^{t-1}}{z}\sum_{\lambda\mid z}1=\sum_{0<\lambda\leqslant P}\sum_{\substack{0<z\leqslant P\\ \lambda\mid z}}\frac{(d(z))^{t-1}}{z}=$$

$$=\sum_{0<\lambda\leqslant P}\frac{(d(\lambda))^{t-1}}{\lambda}\sum_{0<\mu\leqslant P/\lambda}\frac{(d(\mu))^{t-1}}{\mu}\leqslant(c_6(t-1))^2(\log P)^{2^t}.$$

引 理 2·5. 命 t 是一正整數,則

$$\sum_{0<z\leqslant P}(d(z))^t\leqslant c_7(t)P(\log P)^{2^t-1}.$$

證: 由引理 2·4 及歸納法可知

$$\sum_{0<z\leqslant P}(d(z))^t=\sum_{0<z\leqslant P}(d(z))^{t-1}\sum_{\lambda\mid z}1=\sum_{0<\lambda\leqslant P}\sum_{\substack{0<z\leqslant P\\ \lambda\mid z}}(d(z))^{t-1}\leqslant$$

$$\leqslant\sum_{0<\lambda\leqslant P}(d(\lambda))^{t-1}\sum_{0<\mu\leqslant P/\lambda}(d(\mu))^{t-1}=$$

$$=O\Big(\sum_{0<\lambda\leqslant P}(d(\lambda))^{t-1}\frac{P}{\lambda}(\log P)^{2^{t-1}-1}\Big)=O\Big(P(\log P)^{2^t-1}\Big).$$

第 三 章

某些三角和的中值定理(I)

§ 1.

定 理 4. 命 $f(x)$ 代表一個 k 次整值多項式,

$$T(\alpha)=\sum_{x=1}^{P} e(f(x)\alpha).$$

則當 $1\leqslant \nu\leqslant k$ 時,我們有

$$\int_0^1 |T(\alpha)|^{2^\nu}\, d\alpha \leqslant c_1(k,\nu)\, P^{2^\nu-\nu}(\log P)^{c_2(k,\nu)}\, d^{\nu-1}(u),$$

此處 u 是 $f(x)$ 的係數的分子之最大公約數,$c(k,\nu)$ 僅依於 k 及 ν 而與 $f(x)$ 的係數無關.

附記: 因爲

$$g(x)=\log\left(\int_0^1 |T(\alpha)|^{\lambda}\, d\alpha\right)$$

是一凸函數,所以我們可以得出關於任一實數 λ 的不等式. 確切些說: 當 $2^\nu <$ $<\lambda\leqslant 2^{\nu+1}$ 時有不等式

$$\int_0^1 |T(\alpha)|^{\lambda}\, d\alpha\leqslant\left(\int_0^1 |T(\alpha)|^{2^\nu} d\alpha\right)^{2-2^{-\nu}\lambda}\left(\int_0^1 |T(\alpha)|^{2^{\nu+1}} d\alpha\right)^{2^{-\nu}\lambda-1}.$$

因爲本文中以後不引用這一結果,所以我們不證明這一結果.

§2. 關於不等式的若干引理

引 理 3·1. 若 $\alpha+\beta=1$, $\alpha>0$, $\beta>0$ 則

$$s^\alpha t^\beta\leqslant s\alpha+t\beta.$$

證：當 $x>1$，$0<m<1$；我們有

$$x^m-1=m\int_1^x y^{m-1}\,dy\leqslant m\int_1^x dy=m(x-1).$$

取 $x=\frac{s}{t}\ (s>t)$，$m=\alpha$ 及 $1-m=\beta$，卽得引理.

引理 3·2. 若 $\alpha+\beta=1$，$\alpha>0$，$\beta>0$，則對實數 a_n 及 $b_n\ (1\leqslant n\leqslant r)$ 常有

$$\left|\sum_{n=1}^{r}a_nb_n\right|\leqslant\left(\sum_{n=1}^{r}|a_n|^{\frac{1}{\alpha}}\right)^{\alpha}\left(\sum_{n=1}^{r}|b_n|^{\frac{1}{\beta}}\right)^{\beta}.$$

(以後引證時，這不等式將稱爲 Hölder 不等式．而 $\alpha=\beta=\frac{1}{2}$ 的特例，將稱爲 Буняковский, Cauchy 或 Schwarz 不等式).

證：由引理 3·1 可知

$$\frac{\sum_{n=1}^{r}|a_nb_n|}{\left(\sum_{n=1}^{r}|a_n|^{\frac{1}{\alpha}}\right)^{\alpha}\left(\sum_{n=1}^{r}|b_n|^{\frac{1}{\beta}}\right)^{\beta}}=\sum_{n=1}^{r}\left(\frac{|a_n|^{\frac{1}{\alpha}}}{\sum_{n=1}^{r}|a_n|^{\frac{1}{\alpha}}}\right)^{\alpha}\left(\frac{|b_n|^{\frac{1}{\beta}}}{\sum_{n=1}^{r}|b_n|^{\frac{1}{\beta}}}\right)^{\beta}\leqslant$$

$$\leqslant\sum_{n=1}^{r}\left(\frac{\alpha|a_n|^{\frac{1}{\alpha}}}{\sum_{n=1}^{r}|a_n|^{\frac{1}{\alpha}}}+\frac{\beta|b_n|^{\frac{1}{\beta}}}{\sum_{n=1}^{r}|b_n|^{\frac{1}{\beta}}}\right)=\alpha+\beta=1.$$

引理 3·3. 命

$$\underset{y}{\Delta}\,Q(x)=\frac{1}{y}\left(Q(x+y)-Q(x)\right),\quad I=\sum_{x=1}^{P}e(f(x)).$$

今用符號 $\sum_{x}^{P}$ 表示一和*，其項數 $\leqslant c_2(k)P$，x 是變數．則當 $\mu=1,2,\cdots,k$ 時有次之不等式

* 此符號以後將經常採用。

$$|I|^{2^\mu} \leqslant c_3(\mu)\, P^{2^\mu-\mu-1} \sum_{y_1}^{P} \cdots \sum_{y_\mu}^{P} \sum_{x_{\mu+1}}^{P} e\,(y_1 \cdots y_\mu \underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f\,(x_{\mu+1}))\,.$$

證：由等式

$$|I|^2 = \sum_{x_1=1}^{P} \sum_{x_2=1}^{P} e\,(f(x_1) - f(x_2)) =$$

$$= \sum_{x_2}^{P} \sum_{y_1}^{P} e\,(f(x_2+y_1) - f(x_2)) =$$

$$= \sum_{y_1}^{P} \sum_{x_2}^{P} e\,(y_1 \underset{y_1}{\Delta} f(x_2)),$$

可知引理當 $\mu=1$ 時爲眞.

今假定本引理對 $\mu-1$ 爲眞. 用 Cauchy 不等式得出

$$|I|^{2^\mu} = (|I|^{2^{\mu-1}})^2 \leqslant$$

$$\leqslant (c_3(\mu-1))^2\, P^{2(2^{\mu-1}-\mu)} \left| \sum_{y_1}^{P} \cdots \sum_{y_{\mu-1}}^{P} \sum_{x_\mu}^{P} e\,(y_1 \cdots y_{\mu-1} \underset{y_{\mu-1}}{\Delta} \cdots \underset{y_1}{\Delta} f(x_\mu)) \right|^2 \ll$$

$$\ll P^{2^\mu-2\mu}\, P^{\mu-1} \sum_{y_1}^{P} \cdots \sum_{y_{\mu-1}}^{P} \left| \sum_{x_\mu}^{P} e\,(y_1 \cdots y_{\mu-1} \underset{y_{\mu-1}}{\Delta} \cdots \underset{y_1}{\Delta} f(x_\mu)) \right|^2 \ll$$

$$\ll P^{2^\mu-\mu-1} \sum_{y_1}^{P} \cdots \sum_{y_\mu}^{P} \sum_{x_{\mu+1}}^{P} e\,(y_1 \cdots y_\mu \underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1}))\,.$$

引理 3·4. 若 $Q(x)$ 是一 k 次多項式，其最高方次的係數是 α，則 $\underset{y}{\Delta} Q(x)$ 是 x 的 $(k-1)$ 次多項式，其最高方次的係數是 $k\alpha$. 由此推得

$$\underset{y_1}{\Delta} \cdots \underset{y_{k-1}}{\Delta} Q(x) = k!\,\alpha x + B,$$

$$\underset{y_1}{\Delta} \cdots \underset{y_k}{\Delta} Q(x) = k!\,\alpha.$$

此引理的證明十分明顯.

§3. 定理的證明

並不失去普遍性，我們可假定 $f(x)$ 是整係數多項式. 因爲如果 q 是 $f(x)$ 的係數的最小公分母，則由 Hölder 不等式（引理 3·2）可得

$$\int_0^1 |T(\alpha)|^k d\alpha = \int_0^1 \left| \sum_{t=1}^{q} \sum_{x=1}^{[(P-t)/q]} e(f(qx+t)\alpha) \right|^k d\alpha \leqslant$$

$$\leqslant q^{k-1} \sum_{t=1}^{q} \int_0^1 \left| \sum_{x=1}^{[(P-t)/q]} e((f(qx+t)-f(t))\alpha) \right|^k d\alpha,$$

此處 $f(qx+t)-f(t)$ 是整係數多項式. 又注意 $q \leqslant k$！

當 $\nu = 1$ 時此定理顯然眞實. 由引理 3·3 得出

$$|T(\alpha)|^{2^\mu} \ll P^{2^\mu - 1} + P^{2^\mu - \mu - 1} \sum_{y_1}^{P} \cdots \sum_{y_\mu}^{P} \sum_{x_{\mu+1}}^{P}{}^{*} e(y_1 \cdots y_\mu \underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1})\alpha), \tag{1}$$

此處星號 * 代表條件

$$y_1 \cdots y_\mu \underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1}) \neq 0.$$

其中用到由 $y_1 \cdots y_\mu \underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1}) = 0$ 可知有一個 ν 使 $y_\nu = 0$ 或 $\underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1}) = 0$. 因爲 $\underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1})$ 的最高係數非零，所以得出 (1) 式.

以 $|T(\alpha)|^{2^\mu}$ 乘不等式雙方，並且對 α 由 0 至 1 求積分，即得

$$\left.\begin{aligned} &\int_0^1 |T(\alpha)|^{2^{\mu+1}} d\alpha \ll P^{2^\mu - 1} \int_0^1 |T(\alpha)|^{2^\mu} d\alpha + \\ &+ P^{2^\mu - \mu - 1} \int_0^1 \sum_{y_1}^{P} \cdots \sum_{y_\mu}^{P} \sum_{x_{\mu+1}}^{P}{}^{*} e(y_1 \cdots y_\mu \underset{y_\mu}{\Delta} \cdots \underset{y_1}{\Delta} f(x_{\mu+1})\alpha) |T(\alpha)|^{2^\mu} d\alpha. \end{aligned}\right\} \tag{2}$$

由歸納法假定可知 (2) 式右邊的第一項是

$$O(P^{2^\mu - 1} P^{2^\mu - \mu} (\log P)^{c_2(k,\mu)} (d(u))^{\mu-1}) =$$

$$= O(P^{2^{\mu+1} - \mu - 1} (\log P)^{c_2(k,\mu)} (d(u))^{\mu-1}).$$

(2) 式右邊的第二項等於

$$P^{2^\mu-\mu-1}\int_0^1 \sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^{*}\sum_{z_1}^{P}\cdots\sum_{z_{2^\mu}}^{P} e\,((y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1}) -$$

$$-f(z_1)-\cdots-f(z_{2^{\mu-1}})+f(z_{2^{\mu-1}+1})+\cdots+f(z_{2^\mu}))\,\alpha)\,d\,\alpha=$$

$$=P^{2^\mu-\mu-1}R,$$

此處 R 是下列方程式的整數解的組數:

$$\left.\begin{aligned} &y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})=f(z_1)+\cdots+f(z_{2^{\mu-1}})-f(z_{2^{\mu-1}+1})-\cdots-f(z_{2^\mu}),\\ &y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})\neq 0,\quad z_\nu, y_\nu, x_{\nu+1}\ll P.\end{aligned}\right\}\quad(3)$$

對已與的 $z_1,\cdots,z_{2^\mu}$, (3) 式的解數

$$\leqslant d^\mu(f(z_1)+\cdots+f(z_{2^{\mu-1}})-f(z_{2^{\mu-1}+1})-\cdots-f(z_{2^\mu})).$$

由定理 3, 可知

$$R\ll\sum_{z_1}\cdots\sum_{z_{2^\mu}}{}^{**} d^\mu(f(z_1)+\cdots-f(z_{2^\mu}))\ll$$

$$\ll d^\mu(u)\,P^{2^\mu}(\log P)^{c_2(k,\mu)},$$

此處 ** 號表示條件 $f(z_1)+\cdots-f(z_{2^\mu})\neq 0$. 定理已經證明.

§4. Weyl 的引理

引理 3·5. 命 $q>0$,

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\qquad (h,q)=1,$$

及

$$\Omega=\sum_{x=f+1}^{f+q}\min\left(U,\frac{1}{2(\alpha x)}\right).$$

則

$$\Omega<6U+q\log q.$$

證：寫成 $\alpha=\frac{h}{q}+\frac{\theta}{q^2}$，$|\theta|\leqslant 1$．命 $x=x_1+f$；則 $1\leqslant x_1\leqslant q$．把 αf 寫成

$$\alpha f=\frac{b}{q}+\frac{\theta'}{q},\quad |\theta'|\leqslant 1,\quad b:\text{整數},$$

的形式．

由於 $x_1\leqslant q$ 可得

$$\{\alpha x\}=\{\alpha x_1+\alpha f\}=\left\{\frac{hx_1}{q}+\frac{\theta x_1}{q^2}+\frac{b}{q}+\frac{\theta'}{q}\right\}=\left\{\frac{\rho+2\theta''}{q}\right\},\quad |\theta''|\leqslant 1,$$

此處 ρ 表示以 q 除 hx_1+b 所得的絕對值最小的剩餘．

由於 $(h,q)=1$，當 x_1 經過一完整的剩餘系，mod q 時，ρ 經過 0，1，…，$\left[\frac{1}{2}q\right]$，並且同一 ρ 的值出現最多兩次．

Ω 中適合於 $\rho\leqslant 2$ 的各項用 U 代替它們，其他諸項可以表成

$$\rho=2+s,\quad 0<s\leqslant\frac{1}{2}q-2,$$

的形式．因此

$$\left\{\frac{\rho+2\theta''}{q}\right\}>\frac{s}{q}.$$

故知

$$\Omega\leqslant 6U+2\sum_{s=1}^{\frac{1}{2}q-2}\frac{1}{\frac{2s}{q}}<6U+q\log q.$$

引理 3·6 (Weyl)．若 $\alpha_k,\cdots,\alpha_0$ 是實數，

$$f(x)=\alpha_k x^k+\cdots+\alpha_1 x+\alpha_0,$$

$$\left|\alpha_k-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad (h,q)=1,$$

則

$$S=\sum_{x=1}^{P}e(f(x))\ll P^{1+\varepsilon}q^{\varepsilon}\left(\frac{1}{P}+\frac{1}{q}+\frac{q}{P^k}\right)^{2^{1-k}}.$$

證：由引理 3·3 及 3·4，可得

$$|S|^{2^{k-1}} \ll P^{2^{k-1}-k} \sum_{y_1}^{P} \cdots \sum_{y_{k-1}}^{P} \sum_{x_k}^{P} e\,(y_1 \cdots y_{k-1} \underset{y_{k-1}}{\Delta} \cdots \underset{y_1}{\Delta} f(x_k)) \ll$$

$$\ll P^{2^{k-1}-k} \sum_{y_1}^{P} \cdots \sum_{y_{k-1}}^{P} \left| \sum_{x_k}^{P} e\,(k!\, y_1 \cdots y_{k-1} x_k \alpha_k) \right| \ll$$

$$\ll P^{2^{k-1}-k} + P^{2^{k-1}-k} \sum_{y_1}^{P} \cdots \sum_{y_{k-1}}^{P}{}^{*} \left| \sum_{x_k}^{P} e\,(k!\, y_1 \cdots y_{k-1} x_k \alpha_k) \right|,$$

此處 * 表示條件 $y_1 \cdots y_{k-1} \neq 0$． 由引理 1·2 已知

$$k!\, y_1 \cdots y_{k-1} = Y, \quad Y \ll P^{k-1},$$

的解數 $\leqslant (d\,(Y))^{k-1} = O\,(p^{\varepsilon})$，所以

$$|S|^{2^{k-1}} \ll P^{2^{k-1}-1} + P^{2^{k-1}-k+\varepsilon} \sum_{Y}^{P^{k-1}} \left| \sum_{x}^{P} e\,(Y x \alpha_k) \right|.$$

由引理 1·8 可知

$$\sum_{x}^{P} e\,(Yx\alpha_k) \ll \min\left(P, \frac{1}{\{Y\alpha_k\}}\right).$$

又由引理 3·5 可得

$$\sum_{Y}^{P^{k-1}} \min\left(P, \frac{1}{\{Y\alpha_k\}}\right) \ll \left(\frac{P^{k-1}}{q} + 1\right) \max_{t}\left(\sum_{Y=t+1}^{t+q} \min\left(P, \frac{1}{\{Y\alpha_k\}}\right)\right) \ll$$

$$\ll \left(\frac{P^{k-1}}{q} + 1\right)(P + q \log q).$$

由此得出

$$|S|^{2^{k-1}} \ll P^{2^{k-1}-1} + P^{2^{k-1}-k+\varepsilon}\left(\frac{P^{k-1}}{q} + 1\right)(P + q \log q) \ll$$

$$\ll P^{\varepsilon} q^{\varepsilon} P^{2^{k-1}}\left(\frac{1}{P} + \frac{1}{q} + \frac{q}{P^k}\right).$$

第　四　章

某些三角和的中値定理(II)

§ 1.

定 理 5 (定理 B_k). 設 P 是一正整數,

$$C_k = \sum_{x=1}^{P} e(\alpha_k x^k + \cdots + \alpha_1 x).$$

則

$$\int_0^1 \cdots \int_0^1 |C_k|^{\lambda} d\alpha_1 \cdots d\alpha_k \leqslant c(k, \varepsilon) P^{\lambda - \frac{1}{2}k(k+1)+\varepsilon},$$

此處 $\lambda = \lambda(k)$ 的數值由下面的表來定義:

k	2	3	4	5	6	7	8
λ	6	16	46	124	312	760	1778

當 $k = 2$ 時我們有較精密的結果(定理 B_2'):

$$\int_0^1 \cdots \int_0^1 \left| \sum_{x=1}^{P} e(\alpha_2 x^2 + \alpha_1 x) \right|^6 d\alpha_1 d\alpha_2 \leqslant b_1 P^3 (\log P)^3 .$$

此定理的證明依賴於下面的定理:

定 理 6 (定理 A_k). 命

$$f(x) = a_0 x^k + a_1 x^{k-1} + \cdots,$$

此處 a_0 代表一個 $\leqslant b_2(k)$ 的整數, a_1 是一個絕對值不超過 $b_3(k)P$ 的整數. 又命

$$S_k = \sum_{x=1}^{P} e(\alpha_k f(x) + \alpha_{k-2} x^{k-2} + \cdots + \alpha_1 x),$$

則

$$\int_0^1 \cdots \int_0^1 |S_k|^\lambda \, d\alpha_1 \cdots d\alpha_{k-2} \, d\alpha_k \leqslant c_2(k, \varepsilon) P^{\lambda - \frac{1}{2}(k^2-k+2)+\varepsilon},$$

此處 $\lambda = \lambda(k)$ 的數值由下面的表來定義：

k	3	4	5	6	7	8
λ	10	32	86	220	536	1272

這兩條定理的證明互相依賴；就是說，我們用定理 A_{l_1} $(l_1 \leqslant k-1)$ 及 B_{l_2} $(l_2 \leqslant k-1)$ 來證明 A_k；再由定理 A_{l_1} $(l_1 \leqslant k)$ 及 B_{l_2} $(l_2 \leqslant k-1)$ 來證明 B_k. 對不同的 k，方法上略有變化. 當然，如果用歸納法，我們可有一個一致性的方法，但得出的結果稍欠精密. 因此，我們運用這個各階段不相同的方法.

§2. 定理A_k(即定理6)的意義

在定理 A_k 中我們可以取 $f(x) = x^k$. 其證法如次：積分

$$\int_0^1 \cdots \int_0^1 |S_k|^{2\mu} \, d\alpha_1 \cdots d\alpha_k$$

之值等於方程式組

$$f(x_1) + \cdots + f(x_\mu) = f(y_1) + \cdots + f(y_\mu),$$

$$x_1^h + \cdots + x_\mu^h = y_1^h + \cdots + y_\mu^h, \quad 1 \leqslant h \leqslant k-2,$$

$$1 \leqslant x_\nu \leqslant P, \quad 1 \leqslant y_\nu \leqslant P,$$

的整數解答 $x_1, \cdots, x_\mu, y_1, \cdots, y_\mu$ 的組數. 各以 $a_0^{k-1} k^k$, $a_0^h k^h$ $(1 \leqslant h \leqslant k-2)$ 乘以上諸式，即得

$$\sum_{\nu=1}^{\mu} \{(a_0 k x_\nu)^k + k a_1 (a_0 k x_\nu)^{k-1} + \cdots\} = \sum_{\nu=1}^{\mu} \{(a_0 k y_\nu)^k + k a_1 (a_0 k y_\nu)^{k-1} + \cdots\},$$

$$\sum_{\nu=1}^{\mu} (a_0 k x_\nu)^h = \sum_{\nu=1}^{\mu} (a_0 k y_\nu)^h, \quad 1 \leqslant h \leqslant k-2.$$

命 $x_\nu' = a_0 k x_\nu + a_1$ 及 $y_\nu' = a_0 k y_\nu + a_1$, 則得方程組

$$x_1'^k + \cdots + x_\mu'^k = y_1'^k + \cdots + y_\mu'^k,$$

$$x_1'^h + \cdots + x_\mu'^h = y_1'^h + \cdots + y_\mu'^h, \quad 1 \leqslant h \leqslant k-2, \tag{1}$$

但其中

$$k \mid (x_\nu' - a_1), \qquad k \mid (y_\nu' - a_1).$$

由是得出

$$\int_0^1 \cdots \int_0^1 |S_k|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2}\, d\alpha_k \leqslant$$

$$\leqslant \int_0^1 \cdots \int_0^1 \left| \sum_{x=a_1}^{a_0 kP + a_1} e(\alpha_k x^k + \alpha_{k-2} x^{k-2} + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2}\, d\alpha_k \leqslant$$

$$\leqslant 2^{2\mu-1} \left(\int_0^1 \cdots \int_0^1 \left| \sum_{a_1 \leqslant x \leqslant -1} e(\alpha_k x^k + \alpha_{k-2} x^{k-2} + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2}\, d\alpha_k + \right.$$

$$\left. + \int_0^1 \cdots \int_0^1 \left| \sum_{x=0}^{a_0 kP + a_1} e(\alpha_k x^k + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2}\, d\alpha_k \right)^* \ll$$

$$\ll \int_0^1 \cdots \int_0^1 \left| \sum_x^P e(\alpha_k x^k + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2}\, d\alpha_k + 1,$$

此處用上 $a_0 \ll 1$ 及 $a_1 \ll P$. 因之,我們僅需考察 $f(x) = x^k$ 的情況.

§ 3.

我們現在的目的在證明

$$\int_0^1 \cdots \int_0^1 |S_k|^{2k} d\alpha_1 \cdots d\alpha_{k-2}\, d\alpha_k \leqslant b_4(k) P^k L^{k(2^{k-1}-1)},$$

及

$$\int_0^1 \cdots \int_0^1 |C_k|^{2(k+1)} d\alpha_1 \cdots d\alpha_k \leqslant b_5(k) P^{k+1} L^{2^k-1},$$

---

*若 $a_1 > -1$, 則第一個積分毫無所有, 以 0 代之. 又若 $a_0 kP + a_1 < 0$, 則第二個積分也以 0 代之.

此處 $L=\log P$.

引理 4·1. 命

$$s_\nu = x_1^\nu + \cdots + x_k^\nu, \qquad 1 \leqslant \nu \leqslant k.$$

對稱函數

$$f = (s_1 - x_1)\cdots(s_1 - x_k)$$

可以表成 $s_1, \cdots, s_{k-2}$ 及 s_k 的函數而與 s_{k-1} 無關.

證: 命 σ_i 表 $x_1, \cdots, x_k$ 的 i 次初等對稱函數,則

$$f = s_1^k - \sigma_1 s_1^{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k \sigma_k.$$

由與對稱函數有關的一條習知的定理,可得

$$f = (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k\sigma_k + f_1(s_1, \cdots, s_{k-2}). \tag{1}$$

由與對稱函數有關的牛頓定理,可知

$$(-1)^k k\sigma_k = -s_k + \sigma_1 s_{k-1} + (-1)^k \sigma_{k-1}s_1 + f_2(s_1, \cdots, s_{k-2}),$$

及

$$(-1)^{k-1}(k-1)\sigma_{k-1} = -s_{k-1} + f_3(s_1, \cdots, s_{k-2}).$$

由此推得

$$k((-1)^k\sigma_k + (-1)^{k-1}\sigma_{k-1}s_1) =$$

$$= -s_k + \sigma_1 s_{k-1} + (-1)^k\sigma_{k-1}s_1 + (-1)^{k-1}\sigma_{k-1}s_1 - s_1 s_{k-1} + f_4(s_1, \cdots, s_{k-2}) =$$

$$= -s_k + f_4(s_1, \cdots, s_{k-2}). \tag{2}$$

由等式 (1) 及 (2) 可得本引理.

引理 4·2. 命 $k \geqslant 3$. 又命 $s_\nu = \sum_{\mu=1}^{k-1} x_\mu^\nu$, $s_\nu' = \sum_{\mu=1}^{k-1} y_\mu^\nu$. 若 $x_\mu > 0$, $y_\mu > 0$ 及

$$s_k = s_k', \qquad s_\nu = s_\nu', \qquad 1 \leqslant \nu \leqslant k-2,$$

則 $x_1, \cdots, x_{k-1}$ 與 $y_1, \cdots, y_{k-1}$ 之間只有次序的差別.

證：以 σ_ν 及 σ_ν' 各表 $x_1, \cdots, x_{k-1}$ 及 $y_1, \cdots, y_{k-1}$ 的 ν 次初等對稱函數。由牛頓公式可知

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1} \sigma_{k-1} s_1 = 0$$

及

$$s_{k-1} - \sigma_1 s_{k-2} + \cdots + (-1)^{k-1} (k-1) \sigma_{k-1} = 0.$$

同樣的公式對 $y_1, \cdots, y_{k-1}$ 的對稱函數也眞實。由 $s_k = s_k'$ 及當 $1 \leqslant \nu \leqslant k-2$ 時，$s_\nu = s_\nu'$ 及 $\sigma_\nu = \sigma_\nu'$，可得

$$\sigma_1 (s_{k-1} - s'_{k-1}) + (-1)^{k-1} s_1 (\sigma_{k-1} - \sigma'_{k-1}) = 0$$

及

$$s_{k-1} - s'_{k-1} + (-1)^{k-1} (k-1) (\sigma_{k-1} - \sigma'_{k-1}) = 0.$$

消去 $\sigma_{k-1} - \sigma_{k-1}'$ 可知

$$((k-1) \sigma_1 - s_1) (s_{k-1} - s'_{k-1}) = 0.$$

因爲 $(k-1) \sigma_1 - s_1 = (k-2) s_1 \neq 0$，故得

$$s_{k-1} = s'_{k-1}.$$

由此可見 $x_1, \cdots, x_{k-1}$ 是由 $y_1, \cdots, y_{k-1}$ 換位而得者。

引理 4·3.

$$\int_0^1 \cdots \int_0^1 |S|^{2k} d\alpha_1 \cdots d\alpha_{k-2} \, d\alpha_k \leqslant b_4(k) P^k L^{k(2^{k-1}-1)}.$$

證：命 $l = x_1 + \cdots + x_k$. 則由引理 4·2 可知由等式組

$$\left.\begin{aligned} &x_1^k + \cdots + x_k^k = y_1^k + \cdots + y_k^k, \\ &x_1^h + \cdots + x_k^h = y_1^h + \cdots + y_k^h, \qquad 1 \leqslant h \leqslant k-2 \end{aligned}\right\} \qquad (3)$$

得出

$$(l-x_1)\cdots(l-x_k)=(l-y_1)\cdots(l-y_k).$$

對已與的 $y_1, \cdots, y_k$，如

$$(l-y_1)\cdots(l-y_k)\neq 0, \tag{4}$$

則 $x_1, \cdots, x_k$ 的組數最多是

$$d^{k-1}(|(l-y_1)(l-y_2)\cdots(l-y_k)|).$$

因此 (3) 式適合 (4) 的解答之組數(由於引理 2·5)

$$\ll \sum_{y_1}^{P}\cdots\sum_{y_k}^{P} d^{k-1}(|(l-y_1)\cdots(l-y_k)|)\leqslant$$

$$\leqslant \sum_{z_1}^{P}\cdots\sum_{z_k}^{P} d^{k-1}(z_1)\cdots d^{k-1}(z_k)\leqslant$$

$$\leqslant\Big(\sum_{z}^{P} d^{k-1}(z)\Big)^k \ll$$

$$\ll P^k L^{k(2^{k-1}-1)}.$$

又若 (4) 式並不適合，則由

$$(l-x_1)\cdots(l-x_k)=(l-y_1)\cdots(l-y_k)=0$$

可知至少有一 x 與 y 之一相同，不妨假定 $x_k=y_k$. 如是則由引理 4·2 及 (4) 式可知 $x_1, \cdots, x_{k-1}$ 是由 $y_1, \cdots, y_{k-1}$ 換位而得. 適合此條件的解數是 $\ll P^k$. 由此得出本引理.

引 理 4·4. 由等式組

$$x_1^h+\cdots+x_{k+1}^h=y_1^h+\cdots+y_{k+1}^h, \quad 1\leqslant h\leqslant k, \tag{5}$$

可引導出一形如

$$(x_k-y_1)\cdots(x_k-y_k)=(x_{k+1}-y_{k+1})\,g(y_1, \cdots, y_k, x_k, y_{k+1}, x_{k+1})$$

之等式,此處 g 是一 $(k-1)$ 次的齊次各項式;其中含有 x_{k+1}, y_{k+1} 的齊次部分不爲 $x_{k+1}-y_{k+1}$ 所整除,且 g 中 x_{k+1}^{k-1} 的係數不等於 0.

證: 命 $s_\nu=\sum_{i=1}^{k-1}x_i^\nu$ 及 $t_\nu=\sum_{j=1}^{k-1}y_j^\nu$. (5) 式與次式相當

$$s_h=t_h-(x_k^h-y_k^h)-(x_{k+1}^h-y_{k+1}^h),\quad 1\leqslant h\leqslant k. \tag{6}$$

習知

$$s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+(-1)^{k-1}s_{k-1}s_1=0, \tag{7}$$

此處 $\sigma_i=\sigma_i(x_1,\cdots,x_{k-1})$ 是 $x_1,\cdots,x_{k-1}$ 的 i 次初等對稱函數. 習知 σ_1, $\cdots$, σ_{k-1} 是可以由 $s_1,\cdots,s_{k-1}$ 表出來的. 更確切些,我們有

$$s_k-s_1s_{k-1}+\sigma_2(s_1,s_2)s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}(s_1,\cdots,s_{k-1})=0. \tag{8}$$

同法得出

$$t_k-t_1t_{k-1}+\sigma_2(t_1,t_2)t_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}(t_1,\cdots,t_{k-1})=0. \tag{9}$$

將 (6) 式代入 (8) 式之左方而得的函數用 $T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})$ 來表示. 今證明公式

$$T(y_1,\cdots,y_k,x_k,x_{k+1},x_{k+1})=\lambda(x_k-y_1)\cdots(x_k-y_k).$$

此一事實十分明顯,因爲 $T(y_1,\cdots,y_k,x_k,x_{k+1},x_{k+1})$ 對 x_k 而言是一 k 次多項式,且當 $x_k=y_\nu\,(1\leqslant\nu\leqslant k)$ 時此式之值是零.

由此可知

$$T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})-\lambda(x_k-y_1)\cdots(x_k-y_k)$$

是一多項式,當 $x_{k+1}=y_{k+1}$ 時其值是零. 因此

$$T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})=$$
$$=\lambda(x_k-y_1)\cdots(x_k-y_k)+(x_{k+1}-y_{k+1})\,g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1}).$$

最後，在將 (6) 代入 (8) 式之左方時，x_{k+1}, y_{k+1} 的齊次部份的次數是 k，僅其中之第一項所給與的部份是 $x_{k+1}-y_{k+1}$ 的倍數，而非 $(x_{k+1}-y_{k+1})^2$ 的倍數．其他諸項都是 $(x_{k+1}-y_{k+1})^2$ 的倍數．因此得出本引理．

引理 4·5.

$$\int_0^1\cdots\int_0^1|C_k|^{2(k+1)}\,d\alpha_1\cdots d\alpha_k\leqslant b_5(k)P^{k+1}L^{2^k-1}.$$

證：引理中不等式左邊等於方程組

$$\sum_{\nu=1}^{k+1}x_\nu^h=\sum_{\nu=1}^{k+1}y_\nu^h,\qquad 1\leqslant h\leqslant k,\qquad 1\leqslant x,y\leqslant P,\tag{10}$$

的解數．由引理 4·3，可得

$$(x_k-y_1)\cdots(x_k-y_k)=(x_{k+1}-y_{k+1})\,g\,(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1}).\tag{11}$$

若 $(x_k-y_1)\cdots(x_k-y_k)=0$，則 $x_1,\cdots,x_{k+1}$ 乃由 $y_1,\cdots,y_{k+1}$ 換位而得的．方程式有 $O(P^{k+1})$ 個解．

命 n 表一整數 $\neq 0$．且 $n=\lambda_1\cdots\lambda_k=\mu_1\mu_2$．今考察方程組

$$x_k-y_\nu=\lambda_\nu\qquad(1\leqslant\nu\leqslant k),\tag{12}$$

$$x_{k+1}-y_{k+1}=\mu_1\tag{13}$$

及

$$g\,(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})=\mu_2\tag{14}$$

的解數．

若已與 $\lambda_1,\cdots,\lambda_k,\mu_1,\mu_2$ 及 x_k，則由 (12) 式唯一地決定了 $y_1,\cdots,y_k$ 的數值．再由 (13), (14) 及 g 的性質，可知適合 (13), (14) 的 x_{k+1}, y_{k+1} 最多是 k 對．

但對一已知的 n，整數組 $\lambda_1,\cdots,\lambda_k,\mu_1,\mu_2$ 的組數 $\leqslant d^k(n)$．而由已知的 $\lambda_1,\cdots,\lambda_k,\mu_1,\mu_2$ 及 x_k，(10) 式的解數是 $O(1)$．因此，(10) 式的解數

$$\ll\sum_{x_k=1}^{P}\sum_{n}^{P^k}d^k(n)\ll P^{k+1}L^{2^k-1}.$$

此處用了引理 2·5.

§ 4.

引 理 4·6. 命 $g_v(x)$ 是 x 的有整數係數的多項式,

$$g(x)=g_1(x)\alpha_1+\cdots+g_s(x)\alpha_s$$

是一 k 次多項式. 命

$$F=\sum_{x=1}^{P}e^{2\pi i g(x)}.$$

用 Δ^μ 表 $\underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta}$, 則當 $\mu=1, 2, \cdots, k-1$ 時

$$F^{2^\mu}\ll P^{2^\mu-1}+P^{2^\mu-\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^{*}e(y_1\cdots y_\mu\Delta^\mu g(x_{\mu+1})),$$

此處 * 表示下面兩條件之一: (i)

$$y_1\cdots y_\mu\Delta^\mu g_i(X)$$

恆等於零, 或, (ii)

$$y_1\cdots y_\mu\Delta^\mu g_i(x_{\mu+1})\neq 0.$$

證: 此引理可由引理 3·3 推出. 因爲如果 $y_1\cdots y_\mu\Delta^\mu g_i(X)$ 不恆等於零, 則

$$y_1\cdots y_\mu\Delta^\mu g_i(x_{\mu+1})=0$$

的解數 $\ll P^\mu$.

§5. 定 理 的 證 明

B_2 及 B_2' 已由引理 4·5 直接證明.

A_3 的證明. 由引理 4·6 可得

$$|S_3|^4\ll P^3+P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}{}^{*}e(y_1y_2\Delta^2(\alpha_3x_3^3+\alpha_1x_3)).$$

以 $|S_3|^6$ 乘此式兩邊，再對 α_1 及 α_3 各由 0 到 1 積分，可得

$$\int_0^1\int_0^1 |S_3|^{10}\, d\alpha_1\, d\alpha_3 \ll P^3 \int_0^1\int_0^1 |S_3|^6\, d\alpha_1\, d\alpha_3 + PR, \tag{1}$$

此處 R 是方程組

$$y_1 y_2 \Delta^2 x_3^3 = z_1^3 + z_2^3 + z_3^3 - z_4^3 - z_5^3 - z_6^3,$$

$$0 = z_1 + z_2 + z_3 - z_4 - z_5 - z_6, \qquad z \ll P,$$

的解數． 由引理 1·2 可知

$$R \ll \sum_{z_1}^{P} \cdots \sum_{z_5}^{P} d^3\left(z_1^3 + \cdots - z_5^3 - (z_1 + \cdots - z_5)^3\right) \ll P^{5+\varepsilon}.$$

由引理 4·3 及 (1) 可知

$$\int_0^1\int_0^1 |S_3|^{10}\, d\alpha_1\, d\alpha_3 \ll P^{6+\varepsilon}. \tag{2}$$

B_3 的證明． 由引理 4·6，

$$|C_3|^4 \ll P^3 + P \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{x_3}^{P} e\left(y_1 y_2 \Delta^2 (x_3^3 \alpha_3 + x_3^2 \alpha_2)\right). \tag{3}$$

乘以 $|C_3|^8$，再對 $\alpha_1, \alpha_2, \alpha_3$ 各由 0 到 1 求積分，由引理 4·5 可得

$$\int_0^1\int_0^1\int_0^1 |C_3|^{12}\, d\alpha_1\, d\alpha_2\, d\alpha_3 \ll P^{7+\varepsilon} + PR,$$

此處 R 乃方程組

$$y_1 y_2 w = z_1^3 + \cdots - z_8^3,$$

$$2 y_1 y_2 = z_1^2 + \cdots - z_8^2,$$

$$0 = z_1 + \cdots - z_8, \qquad z_\nu \ll P,$$

的解數. $w=\Delta^2 x_3^3 \ll P$.

由引理 4·3, 對固定的 w, 方程組

$$2z_1^3 - wz_1^2 + \cdots - (2z_8^3 - wz_8^2) = 0,$$

$$z_1 + \cdots - z_8 = 0$$

的解數 $\ll P^{5+\varepsilon}$. 而對已知的 $z_1, \cdots, z_8$, 整數 y_1 及 y_2 的對數 $\leqslant d(z_1^2 + + \cdots - z_8^2) = O(P^\varepsilon)$. 故得

$$R \ll \sum_w P^{5+\varepsilon} \ll P^{6+\varepsilon}.$$

因此得出

$$\int_0^1\int_0^1\int_0^1 |C_3|^{12}\, d\alpha_1\, d\alpha_2\, d\alpha_3 \ll P^{7+\varepsilon}. \tag{4}$$

以 $|C_3|^{12}$ 乘 (3) 式,再由 (2) 及 (4) 式可以求出

$$\int_0^1\int_0^1\int_0^1 |C_3|^{16}\, d\alpha_1\, d\alpha_2\, d\alpha_3 \ll P^{10+\varepsilon}.$$

A_4 的證明. 由引理 4·6 可得

$$|S_4|^8 \ll P^7 + P^4 \sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*} c\left(y_1 y_2 y_3 \Delta^3 (x_4^4 \alpha_4 + x_4^2 \alpha_2 + x_4 \alpha_1)\right).$$

乘以 $|S_4|^8$ 再求積分,由引理 4·3 可知

$$\int_0^1\int_0^1\int_0^1 |S_4|^{16}\, d\alpha_1\, d\alpha_2\, d\alpha_4 \ll P^{11+\varepsilon} + P^4 R,$$

此處 R 乃方程組

$$y_1 y_2 y_3 \Delta^3 x_4^4 = z_1^4 + \cdots - z_8^4,$$

$$0 = z_1^2 + \cdots - z_8^2,$$

$$0 = z_1 + \cdots - z_8, \qquad z \ll P,$$

的解數.

依照定理 B_2，由最後二式可知 $z_1, \cdots, z_8$ 的組數是 $\ll P^{8-3+\varepsilon}$. 對固定的 $z_1, \cdots, z_8$，由第一式可知 y_1, y_2, y_3, x_4 的組數是 $\leqslant d^3(z_1^4 + \cdots - z_8^4) = O(P^\varepsilon)$. 因之 $R \ll P^{8-3+\varepsilon} = P^{5+\varepsilon}$, 故

$$\int_0^1\int_0^1\int_0^1 |S_4|^{16}\, d\alpha_1\, d\alpha_2\, d\alpha_4 \ll P^{11+\varepsilon}. \tag{5}$$

重複此種步驟,可得

$$\int_0^1\int_0^1\int_0^1 |S_4|^{24}\, d\alpha_1\, d\alpha_2\, d\alpha_4 \ll P^{18+\varepsilon} \tag{6}$$

及

$$\int_0^1\int_0^1\int_0^1 |S_4|^{32}\, d\alpha_1\, d\alpha_2\, d\alpha_4 \ll P^{25+\varepsilon}. \tag{7}$$

B_4 的證明. 由引理 4·5 顯然有

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{10}\, d\alpha_1\, d\alpha_2\, d\alpha_3\, d\alpha_4 \ll P^{5+\varepsilon}.$$

由引理 4·6,

$$|C_4|^4 \ll P^3 + P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}{}^{*} e\left(y_1 y_2 \Delta^2 (x_3^4\alpha_4 + x_3^3\alpha_3 + x_3^2\alpha_2 + x_3\alpha_1)\right).$$

乘以 $|C_4|^{10}$ 並積分之,可得

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{14}\, d\alpha_1\, d\alpha_2\, d\alpha_3\, d\alpha_4 \ll P^{8+\varepsilon} + PR,$$

此處 R 乃方程組

$$y_1 y_2 \Delta^2 x_3^4 = z_1^4 + \cdots - z_{10}^4,$$

$$y_1 y_2 \Delta^2 x_3^3 = z_1^3 + \cdots - z_{10}^3,$$

$$2\, y_1 y_2 = z_1^2 + \cdots - z_{10}^2,$$

$$0 = z_1 + \cdots - z_{10}$$

的解數．命 $\Delta^2 x_3^3 = 2w$（易見 w 乃 y_1, y_2 及 x_3 的一次式，其係數是整數）．對固定的 w，由 (2) 可知方程組

$$0 = z_1^3 - w z_1^2 + \cdots - (z_{10}^3 - w z_{10}),$$

$$0 = z_1 + \cdots - z_{10}$$

的解數是 $\ll P^{6+\varepsilon}$．因此得出 $R \ll P^{7+\varepsilon}$．故

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{14}\, d\alpha_1\, d\alpha_2\, d\alpha_3\, d\alpha_4 \ll P^{8+\varepsilon}. \tag{8}$$

由引理 4·6，可得

$$|C_4|^8 \ll P^7 + P^4 \sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*} e(y_1 y_2 y_3 \Delta^3 (x_4^4 \alpha_4 + x_4^3 \alpha_3 + x_4^2 \alpha_2 + x_4 \alpha_1)). \tag{9}$$

乘以 $|C_4|^{14}$ 且積分之，可得

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{22}\, d\alpha_1\, d\alpha_2\, d\alpha_3\, d\alpha_4 \ll P^{15+\varepsilon} + P^4 R,$$

此處 R 乃方程組

$$6 y_1 y_2 y_3 w = z_1^4 + \cdots - z_{14}^4,$$

$$6 y_1 y_2 y_3 = z_1^3 + \cdots - z_{14}^3,$$

$$0 = z_1^2 + \cdots - z_{14}^2,$$

$$0 = z_1 + \cdots - z_{14}$$

的解數，此處 $w = \frac{1}{6}\Delta^3 x_4^4$ 乃 y_1, y_2, y_3 及 x_4 的一次式，其係數是整數．易見，R 不超過方程組

$$z_1^4 - w z_1^3 + \cdots - (z_{14}^4 - w z_{14}^3) = 0,$$

$$z_1^2 + \cdots - z_{14}^2 = 0,$$

$$z_1 + \cdots - z_{14} = 0$$

的解數的 $\ll P^{1+\varepsilon}$ 倍. 由引理 4·3 可知

$$R \ll P^{1+\varepsilon} P^{14-4+\varepsilon} \ll P^{11+\varepsilon},$$

及

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{22}\, d\alpha_1 \cdots d\alpha_4 \ll P^{15+\varepsilon}. \tag{10}$$

如法進行但由 (8), (9) 代替引理 4·3, 我們得出

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{22+8\lambda}\, d\alpha_1 \cdots d\alpha_4 \ll P^{15+7\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3. \tag{11}$$

今後將用簡寫法

$$\int f\, dx$$

代替

$$\int_0^1\int_0^1 \cdots \int_0^1 f(x_1, \cdots, x_n)\, dx_1\, dx_2 \cdots dx_n.$$

A_5 的證明. 由引理 4·6,

$$|S_5|^4 \ll P^3 + P \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{x_3}^{P} e(y_1 y_2 \Delta^2 g(x_3)),$$

此處 $g(x_3) = x_3^5\alpha_5 + x_3^3\alpha_3 + x_3^2\alpha_2 + x_3$. 乘以 $|S_5|^{10}$ 且積分,可得

$$\int |S_5|^{14}\, d\alpha \ll P^8 + PR,$$

此處 R 乃方程組*

$$y_1 y_2 \Delta^2 x_3^5 = z_1^5 + \cdots - z_{10}^5,$$

*今後不再重複 w 的定義.

$$2y_1y_2w = z_1^3 + \cdots - z_{10}^3,$$

$$2y_1y_2 = z_1^2 + \cdots - z_{10}^2,$$

$$0 = z_1 + \cdots - z_{10}$$

的解數. 對固定的 w, 由 A_3 可知

$$z_1^3 - wz_1^2 + \cdots - (z_{10}^3 - wz_{10}^2) = 0,$$

$$z_1 + \cdots - z_{10} = 0$$

的解數 $\ll P^{6+\varepsilon}$. 故得出 $R \ll P^{7+\varepsilon}$. 卽得

$$\int |S_5|^{14}\, d\alpha \ll P^{8+\varepsilon}. \tag{12}$$

由引理 4·6,

$$|S_5|^8 \ll P^7 + P^4 \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{y_3}^{P} \sum_{x_4}^{P}{}^{*} e(y_1y_2y_3\Delta^3 g(x_4)).$$

乘以 $|S_5|^{14}$ 且積分,得

$$\int |S_5|^{22}\, d\alpha \ll P^{15+\varepsilon} + P^4 R,$$

此 R 乃方程組

$$y_1y_2y_3\Delta^3 x_3^5 = z_1^5 + \cdots - z_{14}^5,$$

$$6y_1y_2y_3 = z_1^3 + \cdots - z_{14}^3,$$

$$0 = z_1^2 + \cdots - z_{14}^2,$$

$$0 = z_1 + \cdots - z_{14}$$

的解數.

故由 B_2 可知，$R \ll P^{14-3+\varepsilon}$. 由此得出

$$\int |S_5|^{22}\, d\alpha \ll P^{15+\varepsilon}.$$

由引理 4·6,

$$|S_5|^{16} \ll P^{15} + P^{11} \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{y_3}^{P} \sum_{y_4}^{P} \sum_{x_5}^{P}{}^{*} e\left(y_1 y_2 y_3 y_4 \Delta^4 g(x_5)\right).$$

乘以 $|S_5|^{22}$ 且積分，由 B_3 可得

$$\int |S_5|^{38}\, d\alpha \ll P^{30+\varepsilon}. \tag{13}$$

重復此一手續，可得

$$\int |S_5|^{38+16\lambda}\, d\alpha \ll P^{30+15\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3. \tag{14}$$

B_5 的證明. 由引理 4·6 可知

$$|C_5|^8 \ll P^7 + P^4 \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{y_3}^{P} \sum_{x_4}^{P}{}^{*} e\left(y_1 y_2 y_3 \Delta^3 g(x_4)\right).$$

乘以 $|C_5|^{12}$ 且積分，由引理 4·5 可得

$$\int |C_5|^{20}\, d\alpha \ll P^{13+\varepsilon} + P^4 R, \tag{15}$$

此處 R 乃方程組

$$y_1 y_2 y_3 \Delta^3 x_3^5 = z_1^5 + \cdots - z_{12}^5,$$

$$6 y_1 y_2 y_3 w = z_1^4 + \cdots - z_{12}^4,$$

$$6 y_1 y_2 y_3 = z_1^3 + \cdots - z_{12}^3,$$

$$0 = z_1^2 + \cdots - z_{12}^2,$$

$$0 = z_1 + \cdots - z_{12}$$

的解數.

由引理 4·5 得

$$\int |C_5|^{20} \, d\alpha \ll P^{13+\varepsilon}. \tag{16}$$

重複此一步驟,但以 (5), (6), (7) 代替引理 4•5, 可以得出

$$\int |C_5|^{20+8\lambda} \, d\alpha \ll P^{13+7\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3. \tag{17}$$

應用引理 4•6 中 $\mu = 4$ 的情況並用 (10), (11), (12) 及 (13), 可得

$$\int |C_5|^{49+16\lambda} \, d\alpha \ll P^{34+15\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5. \tag{18}$$

A_6 的證明. 應用引理 4·6 中 $\mu = 3$ 的情況,並由引理 4·3, 可得

$$\int |S_6|^{12+8} \, d\alpha \ll P^{13+\varepsilon}.$$

重複此一步驟,並以 (5), (6) 及 (7) 代替引理 4·3, 可得

$$\int |S_6|^{12+8\lambda} \, d\alpha \ll P^{6+7\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4. \tag{19}$$

應用引理 4·6 中 $\mu = 4$ 的情況,並用 B_3, 得出

$$\int |S_6|^{60} \, d\alpha \ll P^{49+\varepsilon}. \tag{20}$$

應用引理 4·6 中 $\mu = 5$ 的情況,並用 B_4, 可得

$$\int |S_6|^{60+32\lambda} \, d\alpha \ll P^{49+31+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5. \tag{21}$$

B_6 的證明. 與 A_6 的證明相似,可得

$$\int |C_6|^{16} \, d\alpha \ll P^{9+\varepsilon} \text{ (此乃引理 4·5 的明顯的推論)},$$

$$\int |C_6|^{16+8\lambda}\,d\alpha \ll P^{9+7\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, \tag{22}$$

$$\int |C_6|^{40+16\lambda}\,d\alpha \ll P^{30+15\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, \tag{23}$$

$$\int |C_6|^{120+32\lambda}\,d\alpha \ll P^{105+31\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, 6. \tag{34}$$

A_7 的證明． 我們有次之式子

$$\int |S_7|^{16}\,d\alpha \ll P^{9+\varepsilon},$$

$$\int |S_7|^{16+8\lambda}\,d\alpha \ll P^{9+7\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, \tag{25}$$

$$\int |S_7|^{40+16\lambda}\,d\alpha \ll P^{30+15\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, \tag{26}$$

$$\int |S_7|^{152}\,d\alpha \ll P^{136+\varepsilon}, \tag{27}$$

$$\int |S_7|^{152+64\lambda}\,d\alpha \ll P^{136+63\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, 6. \tag{28}$$

B_7 的證明． 由引理 4·5, 顯然可得

$$\int |C_7|^{24}\,d\alpha \ll P^{16+\varepsilon}.$$

又得

$$\int |C_7|^{24+8\lambda}\,d\alpha \ll P^{16+7\lambda+\varepsilon}, \qquad \lambda = 1, 2, \tag{29}$$

$$\int |C_7|^{40+16\lambda}\,d\alpha \ll P^{30+15\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, \tag{30}$$

$$\int |C_7|^{120+32\lambda}\,d\alpha \ll P^{105+31\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, 6. \tag{31}$$

$$\int |C_7|^{312+64\lambda}\,d\alpha \ll P^{291+63\lambda+\varepsilon}, \qquad \lambda = 1, 2, 3, 4, 5, 6, 7. \tag{32}$$

A_8 的證明． 由引理 4·6 中 $\mu = 4$ 的情况及 (8) 可得

$$\int |S_8|^{32}\,d\alpha \ll P^{23+\varepsilon}. \tag{33}$$

再用引理 4·6 中 $\mu=3$ 的情況及 A_4 可得

$$\int |S_8|^{40}\, d\alpha \ll P^{30+\epsilon}. \tag{34}$$

同法進行得出

$$\int |S_8|^{40+16\lambda}\, d\alpha \ll P^{30+15\lambda+\epsilon}, \qquad \lambda=1,2,3,4,5, \tag{35}$$

$$\int |S_8|^{120+32\lambda}\, d\alpha \ll P^{105+31\lambda+\epsilon}, \qquad \lambda=1,2,3,4,5,6, \tag{36}$$

$$\int |S_8|^{375}\, d\alpha \ll P^{354+\epsilon}, \tag{37}$$

$$\int |S_8|^{376+128\lambda}\, d\alpha \ll P^{354+127\lambda+\epsilon}, \qquad \lambda=1,2,3,4,5,6,7. \tag{38}$$

B_8 的證明.

$$\int |C_8|^{18+16\lambda}\, d\alpha \ll P^{9+15\lambda+\epsilon}, \qquad \lambda=0,1,2,3,4,5,6, \tag{39}$$

$$\int |C_8|^{114+32\lambda}\, d\alpha \ll P^{99+31\lambda+\epsilon}, \qquad \lambda=1,2,3,4,5,6, \tag{40}$$

$$\int |C_8|^{306+64\lambda}\, d\alpha \ll P^{285+63\lambda+\epsilon}, \qquad \lambda=1,2,3,4,5,6,7, \tag{41}$$

$$\int |C_8|^{754+128\lambda}\, d\alpha \ll P^{726+127\lambda+\epsilon}, \qquad \lambda=1,2,3,4,5,6,7,8. \tag{42}$$

第　五　章

Виноградов 的中值定理及其推論

§1. 定理的敘述

在本章中我們將討論最有名的 Виноградов 定理及其推廣．這一定理是解析數論新研究的一個基本工具．

定 理 7 (Виноградов 的中值定理)．命

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x$$

及

$$C_k = C_k(P) = \sum_{x=1}^{P} e(f(x)).$$

命

$$t_1(k) = t_1 = \begin{cases} \frac{1}{4} k(k+1) + lk, & \text{當 } k \equiv 0, 3 \pmod 4, \\ \frac{1}{4}(k^2 + k + 2) + lk, & \text{當 } k \equiv 1, 2 \pmod 4. \end{cases}$$

則當 $0 \leqslant l \leqslant c_1(k)$ 時，

$$\int_0^1 \cdots \int_0^1 |C_k|^{2t_1} d\alpha_1 \cdots d\alpha_k \leqslant c_2(k) P^{2t_1 - \frac{1}{2}k(k+1) + \delta + \varepsilon},$$

此處

$$\delta = \delta(k) = \frac{1}{2} k(k+1)(1-a)^l, \quad a = 1/k.$$

此定理可以敘述成另一種形式：

上積分的值顯然等於方程組

$$x_1^h + \cdots + x_{t_1}^h = y_1^h + \cdots + y_{t_1}^h, \qquad 1 \leqslant h \leqslant k,$$

$$1 \leqslant x_\nu, y_\nu \leqslant P,$$

的解答 $x_1, \cdots, x_{t_1}; y_1, \cdots, y_{t_1}$ 的組數． 今往證明：對任一整數 T，該積分也等於下列方程組

$$x_1^h + \cdots + x_{t_1}^h = y_1^h + \cdots + y_{t_1}^h, \quad 1 \leqslant h \leqslant k,$$

$$T < x_i, y_i \leqslant T + P,$$

的解答的組數． 命 $X_i = x_i - T$，$Y_i = y_i - T$，則得

$$\sum_{i=1}^{t_1} (X_i + T)^h = \sum_{i=1}^{t_1} (Y_i + T)^h, \qquad 1 \leqslant h \leqslant k.$$

展開此 h 方，易見此方程組與

$$\sum_{i=1}^{t_1} X_i^h = \sum_{i=1}^{t_1} Y_i^h, \quad 1 \leqslant h \leqslant k,$$

完全相當．

又因為 $(0 \leqslant r \leqslant 2t_1)$

$$\int_0^1 \cdots \int_0^1 C_k^r \, \overline{C}_k^{2t_1 - r} \, e^{2\pi i (N_1 \alpha_1 + \cdots + N_k \alpha_k)} \, d\alpha_1 \cdots d\alpha_k$$
$$\leqslant \int_0^1 \cdots \int_0^1 |C_k|^{2t_1} d\alpha_1 \cdots d\alpha_k.$$

故由此定理，可知方程組

$$\sum_{\nu=1}^{r} x_\nu^h - \sum_{\nu=r+1}^{2t_1} y_\nu^h = N_h, \qquad 1 \leqslant h \leqslant k, \qquad 1 \leqslant x, y \leqslant P,$$

的整數解答數

$$\leqslant c_2(k) P^{2t_1 - \frac{1}{2}k(k+1) + \delta + \epsilon}.$$

此定理之證明依於引理 5·1．著者對於證明作了某些簡化及精密化工作．

§2. 引　　理

引理 5·1　命 $P=RH$, $R>1$, $H>1$ 及

$$1\leqslant g_1<g_2<\cdots<g_k\leqslant H,\qquad g_v-g_{v-1}>1,$$

此處 $g_1,\cdots,g_k$ 是整數．又命 x_v 在隔間

$$-\omega+(g_v-1)R\leqslant x_v<-\omega+g_vR,\qquad |\omega|\leqslant P,$$

中變化．則整數組 $x_1,\cdots,x_k$ 中使

$$x_1^h+\cdots+x_k^h,\qquad 1\leqslant h\leqslant k,$$

各在長度 $\leqslant P^{h-1}\,(1\leqslant h\leqslant k)$ 的隔間中的組數

$$\leqslant(2kH)^{\frac{1}{2}k(k-1)}.$$

證：當 $k=1$ 此引理顯然眞實．假定此引理對 $k-1$ 眞實．命 $x_1,\cdots,x_k$ 及 $y_1,\cdots,y_k$ 是適合引理的要求的二整數組．命 $s_h=\sum_{v=1}^{k}x_v^h$，及 $s_h'=\sum_{v=1}^{k}y_v^h$．並以 σ_h 及 σ_h' 各表 $x_1,\cdots,x_k$ 及 $y_1,\cdots,y_k$ 的 h 次初等對稱函數．由引理中的假定，可得

$$|s_h-s_h'|\leqslant P^{h-1},\qquad 1\leqslant h\leqslant k.\tag{2}$$

由 (2) 我們可以證出

$$|\sigma_h-\sigma_h'|\leqslant(2kP)^{h-1},\qquad 1\leqslant h\leqslant k.\tag{3}$$

事實上，當 $h=1$ 時，(3) 式顯然眞實．今假定 (3) 式對 $1,2,\cdots,h-1$ 都眞實．引用關於對稱函數習知之公式

$$s_h-\sigma_1s_{h-1}+\sigma_2s_{h-2}-\cdots-(-1)^hh\sigma_h=0$$

及

$$s_h' - \sigma_1' s_{h-1}' + \sigma_2' s_{h-2}' - \cdots - (-1)^h h \sigma_h' = 0 .$$

由於 $|\sigma_\nu| \leqslant \binom{k}{\nu} P^\nu$, $|s_\nu| \leqslant k P^\nu$, 所以當 $1 \leqslant \nu < h$ 時

$$|\sigma_\nu s_{h-\nu} - \sigma_\nu' s_{h-\nu}'| \leqslant |\sigma_\nu - \sigma_\nu'| \, |s_{h-\nu}| + |\sigma_\nu'| \, |s_{h-\nu} - s_{h-\nu}'| \leqslant$$

$$\leqslant \left((2k)^{\nu-1} k + \binom{k}{\nu} \right) P^{h-1} \leqslant \left(1 + \frac{1}{\nu!}\right)(2k)^{\nu-1} k P^{h-1} .$$

當 $h \geqslant 2$ 時,我們得出

$$\left| \sigma_h - \sigma_h' \right| \leqslant \frac{1}{h}\left(1 + 2k + \frac{3}{2} k \sum_{\nu=2}^{h-1} (2k)^{\nu-1}\right) P^{h-1} {}^{*} \leqslant$$

$$\leqslant \frac{1}{2}\left(1 + \frac{1}{2} k + \frac{3}{2} k \frac{(2k)^{h-1}}{2k-1}\right) P^{h-1} \leqslant \frac{3}{4} (2k)^{h-1} P^{h-1} .$$

對適合 $|X| \leqslant P$ 的 X, 有

$$\Psi(X) = |(X - x_1) \cdots (X - x_k) - (X - y_1) \cdots (X - y_k)| \leqslant$$

$$\leqslant \sum_{h=1}^{k} |\sigma_h - \sigma_h'| \, |X|^{k-h} \leqslant \frac{3}{4} \sum_{h=1}^{k} (2k)^{h-1} P^{k-1} = \frac{3}{4} \frac{(2k)^k}{2k-1} P^{k-1} .$$

由於 $|y_k - x_\nu| \geqslant R \ (\nu = 1, 2, \cdots, k-1)$, 故得出

$$R^{k-1} |y_k - x_k| \leqslant |(y_k - x_1)(y_k - x_2) \cdots (y_k - x_k)| = \Psi(y_k) \leqslant$$

$$\leqslant \frac{3}{4} \frac{(2k)^k}{2k-1} P^{k-1} \leqslant (2kP)^{k-1} .$$

由此可見,適合 (1) 式的 x_k 的個數 $\leqslant (2kH)^{k-1}$. 對一已定的 x_k

---

*當 $h = 2$ 時, 和號 $\sum_{\nu=2}^{1}$ 表零.

$$x_1^h + \cdots + x_{k-1}^h, \qquad 1 \leqslant h \leqslant k-1,$$

各在長度 $\leqslant P^{h-1}\,(1 \leqslant h \leqslant k-1)$ 的隔間中．由歸納法的假定，$x_1, \cdots, x_{k-1}$ 的組數

$$\leqslant (2(k-1)H)^{\frac{1}{2}(k-1)(k-2)}.$$

由於

$$(2(k-1)H)^{\frac{1}{2}(k-1)(k-2)}(2kH)^{k-1} \leqslant (2kH)^{\frac{1}{2}k(k-1)},$$

即得出本引理．

引理 5·2 命 $c \geqslant 1$． 在引理 5·1 的假定下，整數組 $x_1, \cdots, x_k$ 中，使

$$x_1^h + \cdots + x_k^h \qquad (1 \leqslant h \leqslant k)$$

各在長不超過 $cQ^{(1-1/k)h}\ (1 \leqslant h \leqslant k)$ 中的組數不超過

$$(2c)^k (2kH)^{\frac{1}{2}k(k-1)} Q^{\frac{1}{2}(k-1)}.$$

證：把第 h 個隔間分成

$$[c\,Q^{h(1-1/k)}/Q^{h-1}] + 1$$

份，而對每一份都應用引理 5·1． 由於

$$\prod_{h=1}^{k}\left(\left[\frac{c\,Q^{h(1-1/k)}}{Q^{h-1}}\right]+1\right) \leqslant \prod_{h=1}^{k}\left(2c\,Q^{h(1-1/k)-(h-1)}\right) = (2c)^k Q^{\frac{1}{2}(k-1)},$$

所以至多有 $(2Q)^k Q^{\frac{1}{2}(k-1)}$ 組分隔間，其中之任一都適合引理 5·1． 而對每一組分隔間至多有 $(2kH)^{\frac{1}{2}k(k-1)}$ 組解，所以得出本引理．

引理 5·3. 一組整數 $(g_1, \cdots, g_b)$，$1 \leqslant g_v \leqslant H$，如適合次之條件謂之佳位組：其中至少有 k 個，記之為 $g_{i_1}, \cdots, g_{i_k}$，適合

$$g_{i_{v+1}} - g_{i_v} > 1 \qquad (1 \leqslant v \leqslant k-1).$$

非佳位組的個數最多是

$$b!\,3^b H^{k-1}.$$

證：把 $g_1, \cdots, g_b$ 依大小排列

$$1 \leqslant g_1' \leqslant g_2' \leqslant \cdots \leqslant g_b',$$

且命 $f_\nu = g_{\nu+1}' - g_\nu'$. 若此組並非佳位組，則至多有 $k-2$ 個 f 適合 $f_\nu > 1$.

今討論恰有 $\sigma\,(0 \leqslant \sigma \leqslant k-2)$ 個 f 適合 $f_\nu > 1$的組. 此 σ 個 f 的不同位置的個數是 $\binom{b-1}{\sigma}$. 因爲 $0 \leqslant f_\nu \leqslant H-1$ 和 $1 \leqslant g_1' \leqslant H$, 所以不同的組數至多是

$$\binom{b-1}{\sigma} H^{\sigma+1}\, 2^{b-1-\sigma}.$$

故非佳位組的總數將

$$\leqslant \sum_{\sigma=0}^{k-2} \binom{b-1}{\sigma} H^{\sigma+1}\, 2^{b-1-\sigma} \leqslant (1+2)^{b-1} H^{k-1} \leqslant 3^b H^{k-1}.$$

因爲對應於一組固定的 $(g_1', \cdots, g_b')$, $(g_1, \cdots, g_b)$ 的組數是 $b\,!$, 所以得出本引理.

§3. 定 理 的 證 明

引 理 5·4 (遞推公式). 命 b 表一 $\geqslant \frac{1}{4}k(k+1)+k$ 的整數，又命

$$\eta = \left[\frac{1}{k}\frac{\log Q}{\log 2}\right], \qquad a = \frac{1}{k}.$$

則

$$\int_0^1 \cdots \int_0^1 |C_k(Q)|^{2b}\, d\alpha_1 \cdots d\alpha_k \leqslant (7b)^{4b} \max(1, \eta^2)\, Q^{2k-\frac{1}{2}k(k+1)+2(b-k)a} \times$$

$$\times \int_0^1 \cdots \int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\, d\alpha_1 \cdots d\alpha_k.$$

證: 1) 假定 $\eta \geqslant 2$, 命 s 表一適合 $1 \leqslant s \leqslant \eta - 1$ 的整數. 分 $C_k(Q)$ 爲 2^s 部份,每份之長度 $R_s = Q2^{-s}$:

$$C_k(Q) = \sum_{g=1}^{2^s} \sum_{(g-1)R_s < x \leqslant gR_s} e^{2\pi i f(x)} = \sum_{g=1}^{2^s} Z_{sg}, \qquad (\text{定義}).$$

命 $Z = (C_k(Q))^b$. 則

$$Z = \sum^{2^{sb}} Z_{sg_1} \cdots Z_{sg_b}, \tag{1}$$

此處 $\sum^{M}$ 表一和,其項數最多是 M (今後將常有此種了解). 又簡書

$$Z_s = Z_{s;g_1,\cdots,g_b} = Z_{sg_1} \cdots Z_{sg_b}. \tag{2}$$

如果 $g_1, \cdots, g_b$ 成一佳位組, 則 $Z_{s;g_1,\cdots,g_b}$ 稱爲佳位和, 而以 Z_s' 表之. 由引理 5·3, 非佳位的和的個數不超過 $b!\,3^b\,2^{s(k-1)}$. 把非佳位和 Z_s 中的每一因子分爲二份. 如此從一個非佳位和 Z_s 得出 2^b 個和 Z_{s+1}. 由 Z_s 中所得的佳位的 Z_{s+1} 的個數顯然不超過

$$b!3^b2^{s(k-1)} \cdot 2^b = b!6^b2^{s(k-1)}.$$

佳位的 Z_{s+1} 用 Z'_{s+1} 表之. 再如前法,分割非佳位的和. 由於 Z_1 一定是非佳位的,所以我們能夠開始. 重複此項手續,由 $s = 1, 2, \cdots$, 到 $\eta - 1$, 而用 Z_η' 表所有的由非佳位的 $Z_{\eta-1}$ 所獲得的 Z_η. 於是得

$$Z = \sum_{s=1}^{\eta} \sum^{M_s} Z_s', \tag{3}$$

此處 $M_s = b!6^b2^{s(k-1)}$.

2) 由 Schwarz 不等式可得

$$|C_k(Q)|^{2b} = |Z|^2 \leqslant \eta \sum_{s=1}^{\eta} \left| \sum^{M_s} Z_s' \right|^2 \leqslant \eta \sum_{s=1}^{\eta} M_s \sum^{M_s} |Z_s'|^2. \tag{4}$$

我們可假定 $Z'_{s;g_1,\ldots,g_b}$ $(1\leqslant s\leqslant \eta-1)$ 的 $g_1,\cdots,g_k$ 適合引理 5·1 的要求。不然祇須重排足碼卽可。 因爲幾何中項不超過代數中項，所以

$$|Z_{sg_{k+1}}\cdots Z_{sg_b}|^2\leqslant \frac{1}{b-k}\sum_{i=k+1}^{b}|Z_{sg_i}|^{2(b-k)}. \tag{5}$$

把 Z_{sg_i} $(k+1\leqslant i\leqslant b)$ 分成

$$[Q\,2^{-s}/(Q^{1-a}-1)]+1\leqslant Q\,2^{-s}(Q^{1-a}-1)^{-1}+Q^a\,2^{-\eta}\leqslant$$

$$\leqslant Q\,2^{-s}\left(\frac{3}{4}Q^{1-a}\right)^{-1}+Q^a\,2^{-s-1}\leqslant Q^a\,2^{1-s}$$

(因爲 $4\leqslant 2^\eta\leqslant Q^a\leqslant Q^{1-a}$) 部份，每一份的形式是

$$C^*=\sum_x e^{2\pi i f(x)},$$

此處 x 經過一長 $\leqslant Q^a-1$ 的隔間；卽有一整數 ω 存在，使

$$\omega<x\leqslant\omega+Q',\quad 0<Q'\leqslant Q^{1-a},\quad 0\leqslant\omega\leqslant g_iR_s\leqslant Q.$$

利用 Hölder 不等式可知

$$|Z_{sg_i}|^{2(b-k)}\leqslant\left(\sum^{Q^a2^{1-s}}|C^*|\right)^{2(b-k)}\leqslant(Q^a\,2^{1-s})^{2(b-k)-1}\sum^{Q^a2^{1-s}}|C^*|^{2(b-k)}. \tag{6}$$

由 (4), (5) 及 (6) 可得出

$$|Z|^2\leqslant\frac{\eta}{b-k}\sum_{s=1}^{\eta}M_s(Q^a\,2^{1-s})^{2(b-k)-1}\sum^{N_s}|Z_{sg_1}|^2\cdots|Z_{sg_k}|^2\,|C^*|^{2(b-k)}, \tag{7}$$

此處 $N_s=M_s(b-k)Q^a2^{1-s}=b!\,6^5\cdot 2^{s(k-1)}\,(b-k)\,Q^a\,2^{1-s}$. 過 k 維單位方體 $(0\leqslant\alpha_1\leqslant 1,\cdots,0\leqslant\alpha_k\leqslant 1)$ 求積分，得出

$$\int_0^1\cdots\int_0^1|Z|^2\,d\alpha_1\cdots d\alpha_k\leqslant\frac{\eta}{b-k}\sum_{s=1}^{\eta}M_s(Q^a\,2^{1-s})^{2(b-k)-1}\times$$

$$\times \sum^{N_s} \int_0^1 \cdots \int_0^1 |Z_{sg_1}|^2 \cdots |Z_{sg_k}|^2 |C^*|^{2(b-k)} d\alpha_1 \cdots d\alpha_k. \tag{8}$$

3) 積分

$$\int_0^1 \cdots \int_0^1 |Z_{sg_1}|^2 \cdots |Z_{sg_k}|^2 |C^*|^{2(b-k)} d\alpha_1 \cdots d\alpha_k \tag{9}$$

等於下列方程組的解答數:

$$x_1^h + \cdots + x_k^h + y_1^h + \cdots + y_{b-k}^h = x_1'^h + \cdots + x_k'^h + y_1'^h + \cdots + y_{b-k}'^h,$$

$$(1 \leqslant h \leqslant k)$$

此處變數 y 及 y' 在形如

$$\omega < y, y' \leqslant \omega + Q' \qquad (0 < Q' \leqslant Q^{1-a}, \qquad 0 \leqslant \omega \leqslant Q)$$

的隔間中,而 x 及 x' 在隔間

$$(g_i - 1) R_s < x_i, x_i' \leqslant g_i R_s$$

之中,而 $s \leqslant \eta - 1$, 整數 $g_1, \cdots, g_k$ 適合於引理 5·1 的條件.

以 $X + \omega$ 及 $Y + \omega$ 各代 x 及 y. 則 (9) 式也就是方程組

$$X_1^h + \cdots + X_k^h + Y_1^h + \cdots + Y_{b-k}^h = X_1'^h + \cdots + X_k'^h + Y_1'^h + \cdots + Y_{b-k}'^h$$

$$(1 \leqslant h \leqslant k) \tag{10}$$

的解數,此處諸 Y 在隔間 $(0, Q')$ 之中,而 X_i 及 X_i' 在

$$-\omega + (g_i - 1) R_s < X_i, X_i' \leqslant -\omega + g_i R_s \qquad (0 \leqslant \omega \leqslant Q) \tag{11}$$

之中.

若先固定了 X'，則 X 適合於引理 5·2 的條件：其中 $c = 2(b-k)$ 及 $H = 2^s$. 所以 X 及 X' 的組數不超過

$$R_s^k\{4(b-k)\}^k(2k\,2^s)^{\frac{1}{2}k(k-1)}Q^{\frac{1}{2}(k-1)} =$$

$$=\{4(b-k)\}^k(2k)^{\frac{1}{2}k(k-1)}2^{\frac{1}{2}sk(k-1)-sk}Q^{2k-\frac{1}{2}(k+1)}. \tag{12}$$

又對已定的 X 及 X', Y 及 Y' 的組數不超過

$$\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k.$$

$\left(由於 \left|\int_0^1 f(x)\,e^{ixy}\,dx\right| \leqslant \int_0^1 |f(x)|\,dx\right)$. 所以，當 $1\leqslant s\leqslant \eta-1$ 時，

$$\int_0^1\cdots\int_0^1 |Z_{sg_1}\cdots Z_{sg_k}|^2\,|C^*|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k \leqslant$$

$$\leqslant (4(b-k))^k(2k)^{\frac{1}{2}k(k-1)}2^{\frac{1}{2}sk(k+1)-2sk}Q^{2k-\frac{1}{2}(k+1)}\times$$

$$\times\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k. \tag{13}$$

當 $s=\eta$ 時，我們用極顯然的不等式：

$$\int_0^1\cdots\int_0^1 \left|Z_{sg_1}\cdots Z_{sg_k}\right|^2 |C^*|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k \leqslant$$

$$\leqslant R_\eta^{2k}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k. \tag{14}$$

由於 $\eta \geqslant \log Q\,/\,k\log 2 - 1$, $\log 2^\eta \geqslant \log Q^a - \log 2 = \log\frac{1}{2}Q^a$，所以 $Q\,2^{-\eta k}\leqslant 2^k$. 又因為

$$R_\eta^{2k} = Q^{2k}2^{-2k\eta} \leqslant$$

$$\leqslant 2^{-\eta[2k-\frac{1}{2}k(k+1)]}Q^{2k-\frac{1}{2}(k+1)}(Q\,2^{-\eta k})^{\frac{1}{2}(k+1)} \leqslant$$

$$\leqslant 2^{-\eta[2k-\frac{1}{2}k(k+1)]}Q^{2k-\frac{1}{2}(k+1)}2^{\frac{1}{2}k(k+1)},$$

可知 (13) 式對 $s=\eta$ 仍真實.

4) 結合 (8) 及 (13) (當 $s=1,2,\cdots,\eta$), 可得

$$\int_0^1\cdots\int_0^1 |C_k(Q)|^{2b}\,d\alpha_1\cdots d\alpha_k \leqslant \eta\sum_{s=1}^{\eta} M_s\,(Q^a 2^{1-s})^{2(b-k)-1} N_s\,(4(b-k))^k \times$$

$$\times\,(2k)^{\frac{1}{2}k(k-1)}\,2^{\frac{1}{2}sk(k+1)-2sk}\,Q^{2k-\frac{1}{2}k(k+1)}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k \leqslant$$

$$\leqslant \eta c\sum_{s=1}^{\eta} 2^{-s(2b-\frac{1}{2}k(k+1)-2k)}\,Q^{2k-\frac{1}{2}(k+1)+2(b-k)a}\,\times$$

$$\times\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k \leqslant$$

$$\leqslant \eta^2 c\,Q^{2k-\frac{1}{2}(k+1)+2(b-k)a}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k, \tag{15}$$

此處用了不等式 $2b\geqslant\frac{1}{2}k(k+1)+2k$, 式中之

$$c=(b!\,6^b)^2\,2^{2(b-k)}\,(4b)^k\,(2k)^{\frac{1}{2}k(k-1)}.$$

由於

$$c<(12b)^{2b}(4b)^b(2k)^b\leqslant((12b)^2\cdot 4b\cdot 2b)^b\leqslant(7b)^{4b};$$

所以本定理當 $\eta\geqslant 2$ 時眞實.

5) 假定 $\eta<2$. 則

$$\frac{1}{k}\log Q/\log 2<2,\qquad \text{卽 } Q<4^k.$$

把 $C_k(Q)$ 分爲四份,每一份的形式如

$$C^*=\sum_{\omega<x\leqslant\omega+Q'} e^{2\pi i f(x)},\quad \left(0<Q'\leqslant\frac{1}{4}Q\leqslant Q^{1-a}\right).$$

用 Hölder 不等式得出

$$|C_k(Q)|^{2b}\leqslant 4^{2b-1}\sum^{4}|C^*|^{2b}\leqslant 4^{2b-1}Q^{2k(1-a)}\sum^{4}|C^*|^{2(b-k)}.$$

在 k 維單位方體上求積分,得出

$$\int_0^1\cdots\int_0^1 |C_k(Q)|^{2b}\,d\alpha_1\cdots d\alpha_k\leqslant$$

$$\leqslant 4^{2b-1}Q^{2k(1-a)}\sum^{4}\int_0^1\cdots\int_0^1 |C^*|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k\leqslant$$

$$\leqslant 4^{2b}Q^{2k(1-a)}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k\leqslant$$

$$\leqslant 4^{2b}Q^{2b-\frac{1}{2}k(k+1)+2(b-k)a}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k,$$

此處用了 $2b>\frac{1}{2}k(k+1)$. 故得出引理 5·4.

定 理 7′. 仍如定理 7 的假定,若 $s\geqslant\frac{1}{4}k(k+1)+lk$, 則

$$\int_0^1\cdots\int_0^1 |C_k(P)|^{2s}\,d\alpha_1\cdots d\alpha_k\leqslant(7s)^{4sl}(\log P)^{2l}P^{2s-\frac{1}{2}k(k+1)+\delta}.$$

這定理顯然是定理 7 的更精密的形式.

證: 如命 $P^{1-a}\leqslant 3$, 則 $P\leqslant 9$, 而本定理毋須證明. 我們假定 $P^{1-a}>3$. 則 $P>e$.

當 $l=0$ 時,定理顯然眞實. 今在 l 上用歸納法. 假定此結論對 $l-1$ 眞實. 由引理 5·4 可知

$$\int_0^1\cdots\int_0^1 |C_k(P)|^{2s}\,d\alpha_1\cdots d\alpha_k\leqslant(7s)^{4s}P^{2k-\frac{1}{2}(k+1)+2(s-k)a}\times$$

$$\times(\log P)^2\int_0^1\cdots\int_0^1 |C_k(P^{1-a})|^{2(s-k)}\,d\alpha_1\cdots d\alpha_k. \tag{16}$$

用歸納法的假定,取 $l-1$, $s-k$ 及 P^{1-a} 代替 l, s 及 P, 可知當 $P^{1-a}>3>2$ 時,

$$\int_0^1\cdots\int_0^1 |C_k(P^{1-a})|^{2(s-k)}\,d\alpha_1\cdots d\alpha_k\leqslant(7s)^{4s(l-1)}(\log P)^{2(l-1)}\times$$

$$\times P^{(1-a)(2s-2k-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)(1-a)^{l-1})}. \tag{17}$$

由 (16) 及 (17) 總結出本定理.

§4. 定理推論之一

定理 8. 命 $P \geqslant 2$, $s \geqslant \frac{1}{4}k(k+1)+lk$. 又命 $f(x)$ 表一 k 次的整值多項式,則

$$\int_0^1 \left| \sum_{x=1}^{P} e(\alpha f(x)) \right|^{2s} d\alpha \ll (\log P)^{2l} P^{2s-k+\delta},$$

此處

$$\delta = \frac{1}{2}(1-a)^l k(k+1).$$

證: 如第三章定理 4 的證明,我們可以假定 $f(x)$ 是一整係數多項式:

$$f(x) = A_k x^k + \cdots + A_1 x + A_0.$$

方程

$$f(x_1) + \cdots + f(x_s) = f(y_1) + \cdots + f(y_s), \quad 1 \leqslant x, y \leqslant P,$$

的整數解之組數顯然等於方程組

$$x_1^h + \cdots + x_s^h - y_1^h - \cdots - y_s^h = N_h, \quad 1 \leqslant h \leqslant k, \tag{1}$$

的解數,此處 $N_1, \cdots, N_k$ 適合於

$$A_k N_k + \cdots + A_1 N_1 = 0, \quad N_h \ll P^h. \tag{2}$$

(注意 $x_1, \cdots, x_s, y_1, \cdots, y_s, N_1, \cdots, N_k$ 都視爲未知數).

由於 $N_h \ll P^h$, 所以有

$$\ll P^{1+2+\cdots+k-1} \ll P^{\frac{1}{2}k(k-1)}$$

組 $N_1, \cdots, N_k$ 適合 (2) 式,因爲 N_k 是由 $N_1, \cdots, N_{k-1}$ 唯一地决定.

對固定的 $N_1, \cdots, N_{k-1}$ 及 N_k, (1) 式的解數等於

$$\int_0^1\cdots\int_0^1\left|\sum_{x=1}^{P}e(\alpha_k x^k+\cdots+\alpha_1 x)\right|^{2s}e(-(N_k\alpha_k+\cdots+N_1\alpha_1))\,d\alpha_1\cdots d\alpha_k.$$

由定理 7′、此積分

$$\leqslant\int_0^1\cdots\int_0^1\left|\sum_{x=1}^{P}e(\alpha_k x^k+\cdots+\alpha_1 x)\right|^{2s}d\alpha_1\cdots d\alpha_k\leqslant$$

$$\leqslant(7s)^{4sl}(\log P)^{2l}P^{2s-\frac{1}{2}k(k+1)+\delta}.$$

§5. 單和與平均值之間的關係

引理 5·5. 命 $\tau\geqslant 1$ 及

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{\tau}{q^2},\quad (h,q)=1,$$

則適合不等式

$$\{\alpha y\}\leqslant\frac{V}{q},\quad f\leqslant y\leqslant f+N,$$

的整數 y 的個數

$$\leqslant 2(V+2\tau)\left(\frac{N}{q}+1\right).$$

證：若能證明適合

$$\{\alpha y\}\leqslant\frac{V}{q},\quad f\leqslant y\leqslant f+q,\tag{1}$$

的整數 y 的個數 $\leqslant 2(V+2\tau)$，則本引理卽已證明．今寫

$$y=f+z,\quad \alpha=\frac{h}{q}+\frac{\tau\vartheta}{q^2},\quad |\vartheta|\leqslant 1,$$

則

$$\alpha y=\frac{hz}{q}+\frac{\tau\vartheta z}{q^2}+\frac{hf}{q}+\frac{\tau\vartheta f}{q^2}=$$

$$=\frac{hz+[c]+(c-[c])+\tau\vartheta z/q}{q},\quad\left|\frac{\tau\vartheta z}{q}\right|\leqslant\tau,$$

此處 $c = hf + \tau\vartheta f/q$.

如果 $q \leqslant 2(V + 2\tau)$, 定理顯然眞實. 當 z 經過一完全剩係系, $\bmod q$, 則 $w = hz + [c]$ 也是如此. 所以

$$\alpha y = \frac{w + \sigma(w)}{q},$$

此處

$$-\tau \leqslant c - [c] - \tau \leqslant \sigma(w) \leqslant c - [c] + \tau < 1 + \tau.$$

適合不等式

$$V + \tau \leqslant w < q - \tau - V - 1 \tag{2}$$

的 w 顯然也適合不等式

$$\frac{V}{q} \leqslant \frac{w + \sigma(w)}{q} < 1 - \frac{V}{q}.$$

而這並不適合 (1) 式. 適合 (2) 的整數 w 的個數 $\geqslant q - 2V - 2\tau - 2$, 所以適合 (1) 的整數的個數

$$\leqslant q - (q - 2V - 2\tau - 2) = 2V + 2\tau + 2 \leqslant 2(V + 2\tau).$$

引理 5·6. 命 $Y \geqslant 1$. 又命 $A_0, A_1, \cdots, A_{k-1}$ 是適合

$$A_0 = 1, \quad |A_r| \leqslant (r + 1)Y^r$$

的整數. 則由方程組

$$v_r = \sum_{s=r}^{k} \binom{s+1}{r} A_{s-r} u_s \tag{3}$$

可以解得 $(k + 1)k \cdots (r + 1)u_r$ 是 $v_1, \cdots, v_r$ 的線性式, 其係數都是整數, 即

$$(k + 1)k \cdots (r + 1)u_r = \sum_{s=r}^{k} a_{rs} v_s, \tag{4}$$

且

$$a_{rs} = O\,(Y^{s-r}).$$

證：當 $r = k$ 時，這引理顯然眞實．假定對 $k,\ k-1,\ \cdots,\ r+1$ 時，這引理都眞實．由 (3) 式可知

$$(k+1)\cdots(r+1)\,u_r = (k+1)\cdots(r+2)\left(v_r - \sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\,u_s\right) =$$

$$= (k+1)\cdots(r+2)\,v_r - \sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\,\frac{s!}{(r+1)!}\,(k+1)\cdots(s+1)\,u_s =$$

$$= (k+1)\cdots(r+2)\,v_r - \sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\,\frac{s!}{(r+1)!}\sum_{s\leqslant u\leqslant k}a_{su}\,v_u.$$

當 $k \geqslant u > r$ 時，

$$a_{ru} = \sum_{r+1\leqslant s\leqslant u}\binom{s+1}{r}A_{s-r}\,\frac{s!}{(r+1)!}\,a_{su}$$

顯然是一整數，且

$$a_{ru} = O\Big(\sum_{r+1\leqslant s\leqslant u}|A_{s-r}|\,|a_{su}|\Big) =$$

$$= O\,(Y^{s-r}\cdot Y^{u-s}) = O\,(Y^{u-r}).$$

當 $u = r$ 時，顯然

$$a_{rr} = O\,(1).$$

引理 5·7. 命 $\xi_1,\ \cdots,\ \xi_n$ 表實數．則對整數 $l_1,\ \cdots,\ l_n$ 我們有不等式

$$\left\{\sum_{i=1}^{n} l_i\,\xi_i\right\} \leqslant \sum_{i=1}^{n}|l_i|\,\{\xi_i\}.$$

這引理是下面不等式的推理：

$$\{\xi_1 \pm \xi_2\} \leqslant \{\xi_1\} + \{\xi_2\}.$$

引理 5·8. 命 $\alpha_k, \cdots, \alpha_1$ 是實數,

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x.$$

假定我們有以下的事實: 命 $0 < \delta_1 < 1$, T 是任意整數, 則

$$\int_0^1 \cdots \int_0^1 \left| \sum_{x=T+1}^{T+P} e(f(x)) \right|^{2t_1} d\alpha_1 \cdots d\alpha_k = O\left(P^{2t_1 - \frac{1}{2}k(k+1) + \delta_1}\right), \tag{5}$$

此處符號 O 所包含的常數依於 t_1, δ_1 及 k, 但將來事實上 t_1, δ_1 都是 k 的函數. 在這樣的假定下我們有:

命 $\beta_{k+1}, \cdots, \beta_1$ 表實數,

$$F(x) = \beta_{k+1} x^{k+1} + \cdots + \beta_1 x.$$

又命 r 是適合於 $2 \leqslant r \leqslant k+1$ 的整數. 假定

$$\left| \beta_r - \frac{h}{q} \right| \leqslant \frac{1}{q^2}, \quad (h, q) = 1, \quad 1 \leqslant q \leqslant P^r, \tag{6}$$

則對任一 T, 我們有

$$S = \sum_{x=T+1}^{T+P} e(F(x)) = O\begin{cases} (P^{1-\rho}) & \text{當 } \frac{1}{2}P \leqslant q \leqslant P^{r-1}, \\ \left(P^{1-\rho}\left(\frac{q}{P^{r-1}}\right)^{\frac{1}{2t_1+k+1}}\right) & \text{當 } P^{r-1} \leqslant q \leqslant P^r, \end{cases}$$

此處

$$\rho = \frac{1-\delta_1}{2t_1 + k - 1}.$$

證: (這一重要技巧是 Виноградов 所發明的). 當 $0 < y \leqslant Y < P$ 時, 命

$$S_0 = \sum_{x=T+1}^{T+P} e(F(x+y) - F(y)) = \sum_{x=T+1}^{T+P} e(\phi(x)),$$

此處

$$\phi(x) = Y_1 x + \cdots + Y_{k+1} x^{k+1},$$

$$Y_j = Y_j(y) = \frac{1}{j!}\frac{d^j}{dy^j}F(y) =$$

$$= \binom{k+1}{j}\beta_{k+1}y^{k+1-j} + \cdots + \binom{j+1}{j}\beta_{j+1}y + \beta_j. \tag{7}$$

顯然有

$$|S_0| = |S| + 2\vartheta y, \qquad |\vartheta| \leqslant 1.$$

因此

$$|S| \leqslant Y^{-1}\sum_{y=1}^{Y}|S_0| + Y.$$

用 Hölder 不等式兩次，有

$$|S|^{2t_1} \leqslant 2^{2t_1-1}\left(\left(Y^{-1}\sum_{y=1}^{Y}|S_0|\right)^{2t_1} + Y^{2t_1}\right) =$$

$$= O\left(Y^{-1}\sum_{y=1}^{Y}|S_0|^{2t_1} + Y^{2t_1}\right). \tag{8}$$

命

$$S_1 = \sum_{x=T+1}^{T+P} e(\alpha_1 x + \cdots + \alpha_k x^k + \beta_{k+1}x^{k+1}).$$

對一固定的 y, $Y_1, \cdots, Y_k$ 也定. 今討論適合於

$$\{\alpha_1 - Y_1\} \leqslant \frac{1}{2}P^{-2}Y, \cdots, \ \{\alpha_k - Y_k\} \leqslant \frac{1}{2}P^{-k-1}Y, \quad 0 \leqslant \alpha_i < 1,$$

的實數組 $\alpha_1, \cdots, \alpha_k$. 如此所得出的 $(\alpha_1, \cdots, \alpha_k)$ 所成之域，用 $\Omega(y)$ 表它. 如果 $(\alpha_1, \cdots, \alpha_k)$ 在 $\Omega(y)$ 中，則

$$S_0 = S_1 + O(Y),$$

即得

$$|S_0|^{2t_1} = O(|S_1|^{2t_1}) + O(Y^{2t_1}). \tag{9}$$

聯合 (8) 及 (9)，可知

$$|S|^{2t_1} = O(|S_1|^{2t_1}) + O(Y^{2t_1}).$$

積分等式兩邊，其積分區域是 $\Omega(y)$，則得

$$|S|^{2t_1} = O\left(P^{\frac{1}{2}k(k+1)+k} Y^{-k} \int_{\Omega(y)} \cdots \int |S_1|^{2t_1} d\alpha_1 \cdots d\alpha_k\right) + O(Y^{2t_1}), \tag{10}$$

此處用上了

$$\int_{\Omega(y)} \cdots \int d\alpha_1 \cdots d\alpha_k \gg \prod_{i=1}^{k} (P^{-(i+1)} Y) = P^{-\frac{1}{2}k(k+1)-k} Y^k.$$

今往計算：有多少個不同的 y，使 $\Omega(y)$ 皆包有一固定的點．若 $\Omega(y)$ 及 $\Omega(y_0)$ 有一公共點，則

$$\{Y_r(y) - Y_r(y_0)\} \leqslant P^{-r-1} Y, \quad 1 \leqslant r \leqslant k.$$

命 $v_r = Y_r(y) - Y_r(y_0)$， $u_s = \beta_{s+1}(y - y_0)$ 及

$$A_{s-r} = \frac{y^{s-r+1} - y_0^{s-r+1}}{y - y_0}.$$

由 (7) 可知

$$v_r = \sum_{r \leqslant s \leqslant k} \binom{s+1}{r} \beta_{s+1} (y^{s-r+1} - y_0^{s-r+1}) =$$

$$= \sum_{r \leqslant s \leqslant k} \binom{s+1}{r} A_{s-r} u_s.$$

由引理 5·6 及 5·7 可知，當 $1 \leqslant r < k$ 時

$$\left\{\frac{(k+1)!}{r!} u_r\right\} \leqslant \sum_{r \leqslant s \leqslant k} |a_{rs}| \{v_s\} =$$

$$= O\Big(\sum_{r\leqslant s\leqslant k} Y^{s-r} P^{-s-1} Y\Big) =$$

$$= O(Y P^{-r-1}).$$

以 r 代 $r-1$，則得，當 $2 \leqslant r < k+1$ 時

$$\left\{\frac{(k+1)!}{(r-1)!}\beta_r(y-y_0)\right\} = O(Y P^{-r}), \tag{11}$$

此處

$$1 \leqslant y \leqslant Y. \tag{12}$$

由引理 5·5，可知適合 (11) 及 (12) 的 y 的個數是

$$O\left(\left(\frac{Yq}{P^r}+1\right)\left(1+\frac{Y}{q}\right)\right) = O\left(\frac{Yq}{P^r}+1\right) = O\left(\frac{q}{P^{r-1}}+1\right).$$

(因爲 $q \geqslant \frac{1}{2}P$ 及 $Y \leqslant P$)．

故 k 維單位方體

$$0 \leqslant \alpha_1 \leqslant 1, \cdots, \quad 0 \leqslant \alpha_k \leqslant 1$$

中每一點 $(\alpha_1, \cdots, \alpha_k)$ 最多爲 $O\left(\frac{q}{P^{r-1}}+1\right)$ 個 $\Omega(y)$ $(y=1, \cdots, Y)$ 所蓋上．所以由 (10) 可知

$$|S|^{2t_1} = O\Big(P^{\frac{1}{2}k(k+1)+k}\frac{1}{Y}\sum_{y=1}^{Y}\int\cdots\int_{\Omega(y)} |S_1|^{2t_1}\, d\alpha_1\cdots d\alpha_k\Big) + O(Y^{2t_1}) =$$

$$= O\left(P^{\frac{1}{2}k(k+1)+k}\, Y^{-k-1}\left(\frac{q}{P^{r-1}}+1\right)\int_0^1\cdots\int_0^1 |S_1|^{2t_1}\, d\alpha_1\cdots d\alpha_k\right) +$$

$$+ O(Y^{2t_1}).$$

由

$$\int_0^1\cdots\int_0^1 |S_1|^{2t_1}\, d\alpha_1\cdots d\alpha_k \leqslant \int_0^1\cdots\int_0^1 \Big|\sum_{x=T+1}^{T+P} e(f(x))\Big|^{2t_1} d\alpha_1\cdots d\alpha_k$$

及 (6) 式可知

$$|S|^{2t_1}=O\left(P^{\frac{1}{2}k(k+1)+k}\,Y^{-k-1}\left(\frac{q}{P^{r-1}}+1\right)P^{2t_1-\frac{1}{2}k(k+1)+\delta_1}\right)+O(Y^{2t_1})=$$

$$=O\left(P^{2t_1+k+\delta_1}\,Y^{-k-1}\left(\frac{q}{P^{r-1}}+1\right)\right)+O\left(Y^{2t_1}\right).$$

取

$$Y=\begin{cases}\left[P^{1-\frac{1-\delta_1}{2t_1+k+1}}\right]+1 & \text{當 } \frac{P}{2}\leqslant q\leqslant P^{r-1},\\ \left[P^{1-\frac{1-\delta_1}{2t_1+k+1}}\left(\frac{q}{P^{r-1}}\right)^{\frac{1}{2t_1+k+1}}\right]+1 & \text{當 } P^{r-1}\leqslant q\leqslant P^{r},\end{cases}$$

即得出引理.

引理 5·9. 與引理 5·8 的假定相同,當 $1\leqslant q\leqslant P$ 時

$$S=\sum_{x=T+1}^{T+P}e(F(x))=O(P\,q^{-\rho}).$$

證: 分此和爲不多於 P/q 個部分,其中任一部分的長 Q 適合於 $q\leqslant Q\leqslant 2q$ 由引理 5·8 可知

$$|S|\leqslant\frac{P}{q}\max_{t}\left|\sum_{x=t+1}^{t+Q}e(F(x))\right|=O\left(\frac{P}{Q}\cdot Q^{1-\rho}\right)=O(P\,q^{-\rho}).$$

§6. 定理推論之二(三角和的估值)

定理 9. 用下面的表來定義 σ_k 的數值:

k	2	3	4	5	6	7	8	$\geqslant 9$
σ_k	4	9	20	51	130	319	768	$2k^2(2\log k+\log\log k+3)$

命 $2\leqslant r\leqslant k$,

$$\left|\alpha_r-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\qquad (h,q)=1,\qquad 1\leqslant q\leqslant P^r; \tag{1}$$

又命

$$f(x)=\alpha_k x^k+\cdots+\alpha_1 x.$$

則

$$\sum_{x=1}^{P} e(f(x))=\begin{cases} O\left(P^{1-\frac{1}{\sigma_k}+\varepsilon}\right) & \text{當 } P\leqslant q\leqslant P^{r-1}, \quad (2)\\ O\left(Pq^{-\frac{1}{\sigma_k}+\varepsilon}\right) & \text{當 } 1\leqslant q\leqslant P. \quad (3)\end{cases}$$

證：當 $k\leqslant 11$，這結果可由引理 5·8 及 5·9（其中 $\delta_1=\varepsilon$, $\sigma_k=2t_1+k+1$）及定理 5 直接推出．

當 $k>11$ 時，我們應用引理 5·8（其中 $\delta_1=\delta(k-1)$，而 δ 的定義見定理 7）．由定理 7 可知

$$\frac{1}{\rho}=\left(2t_1(k-1)+k\right)\Big/\left(\left(1-\frac{1}{2}k(k-1)\right)\left(1-\frac{1}{k-1}\right)^l\right)\leqslant$$

$$\leqslant\left(\frac{1}{2}k^2+2lk\right)\Big/\left(1-\frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l\right)\leqslant$$

$$\leqslant\left(\frac{1}{2}k^2+2lk\right)\left(1+k^2(1-\frac{1}{k})^l\right). \tag{4}$$

在證明這不等式時，我們假定了：

$$\frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l\leqslant\frac{1}{2}, \tag{5}$$

並應用了：當 $0\leqslant x\leqslant\frac{1}{2}$，則 $(1-x)^{-1}\leqslant 1+2x$．取

$$l=\left[\frac{2\log k+\log\log k}{-\log(1-1/k)}\right]+1,$$

則

$$l<k(2\log k+\log\log k)+1$$

及

$$k^2\left(1-\frac{1}{k}\right)^l \leqslant \frac{1}{\log k}, \tag{6}$$

此處用上了

$$\frac{1}{-\log(1-1/k)} = \left(\frac{1}{k}+\frac{1}{2k^2}+\frac{1}{3k^3}+\cdots\right)^{-1} \leqslant k.$$

而 (6) 也同時說明了 (5) 的正確性.

所以當 $k \geqslant 9$ 時,有

$$\frac{1}{\rho} \leqslant \left(\frac{1}{2}k^2 + 2k^2(2\log k + \log\log k) + 2k\right)\left(1+\frac{1}{\log k}\right) \leqslant$$

$$\leqslant 2k^2\left(2\log k + \log\log k + \frac{1}{4} + \frac{1}{k} + \frac{\log\log k}{\log k} + \frac{1}{4\log k} + \frac{1}{k\log k} + 2\right) \leqslant$$

$$\leqslant 2k^2(2\log k + \log\log k + 3).$$

這證明了 (2) 式.

同樣的方法,但用引理 5·9 代替引理 5·8, 我們可以得出 (3) 式.

定理 5 及引理 5·8 的另一推理如次:

引理 5·10. 設 $k < 9$, 則在定理 9 的條件下,當 $P^{r-1} \leqslant q \leqslant P^r$ 時, 有

$$\sum_{x=1}^{P} e^{2\pi i f(x)} \ll P^{1-\frac{1}{\sigma_k}+\varepsilon}\left(\frac{q}{P^{r-1}}\right)^{\frac{1}{\sigma_k}}.$$

當 $k \geqslant 9$ 時, 目前我們不能獲得出如此精確的結果. 但為了以後的應用, 我們先給與如下的初步的結果:

引理 5·11. 設 $k \geqslant 9$, 則在定理 9 的條件下, 當 $P^{r-1} \leqslant q \leqslant P^{r-1k}$ 時, 有

$$\sum_{x=1}^{P} e^{2\pi i f(x)} \ll P^{1-1/\rho'}, \qquad \rho' = 60\, k^3 \log k.$$

證：由引理 5·8 我們知道

$$\sum_{x=1}^{P} e^{2\pi i f(x)} \ll P^{1-\rho}\left(P^{1-\frac{1}{4k}}\right)^{\frac{1}{2t_1+k+1}} \ll$$

$$\ll P^{1-\frac{1/4k-\delta_1}{2t_1+k+1}},$$

此處 $\delta_1 = \delta(k-1)$． 取

$$l = \left[\frac{4\log k}{-\log(1-1/k)}\right] + 1,$$

則

$$l \leqslant 4k\log k + 1$$

及

$$\delta_1 \leqslant k^2\left(1-\frac{1}{k}\right)^l \leqslant \frac{1}{k^2}.$$

亦如證明 (4) 式，可得

$$(2t_1(k-1)+k+1)\Big/\left(\frac{1}{4k}-\delta_1\right) \leqslant$$

$$\leqslant \left(\frac{1}{2}k^2 + 2lk\right)\Big/\left(\frac{1}{4k}-\frac{1}{k^2}\right) \leqslant$$

$$\leqslant \left(\frac{1}{2}k^2 + 8k^2\log k + 2k\right) 4k\left(1-\frac{4}{k}\right)^{-1} \leqslant$$

$$\leqslant 4k^3\log k\left(8+\frac{1}{2\log k}+\frac{2}{k\log k}\right)\left(1-\frac{4}{k}\right)^{-1} \leqslant$$

$$\leqslant 4k^3\log k\left(8+\frac{13}{18\log 9}\right)\left(\frac{9}{5}\right) <$$

$$< 60\,k^3\log k.$$

附記：較引理 5·12 更完整的結果如下：當 $k \leqslant 9$ 及 $P^{r-1} \leqslant q \leqslant P^r$ 時，

$$\sum_{x=1}^{P} e^{2\pi i f(x)} \ll P^{1-1/\sigma'} \left(\frac{q}{P^{r-1}}\right)^{1/\sigma'},$$

此處

$$\sigma' = k^3 (3 \log k + \log \log k + 5).$$

這一結果可由以後證明的定理 16 推出之.

第 六 章

含有素數變數的三角和

§ 1.

本章的目的在證明定理 10，這是堆壘素數論的基本工具． 定理 10 基本上是 И. М. Виноградов* 所創造的，今僅作若干必要的擴充，使其能夠適合地用到本書所討論的問題． 我們常以 L 代表 $\log P$.

定 理 10. 命 $0 < Q \leqslant c_1(k) L^{\sigma_1}$ 及

$$S = \sum_{\substack{p \leqslant P \\ p \equiv l \pmod{Q}}} e(f(p)),$$

式中

$$f(x) = \frac{h}{q} x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k, \qquad (h, q) = 1,$$

而 α 是實數． 並設 $L^\sigma < q \leqslant P^k L^{-\sigma}$． 對任一 $\sigma_0 > 0$，當 $\sigma \geqslant 2^{6k}(\sigma_0 + \sigma_1 + 1)$ 時，常有

$$|S| \leqslant c_2(k) P L^{-\sigma_0} Q^{-1}.$$

§ 2. 若干必要的引理

引 理 6·1. 當 $\sigma_2 \leqslant 2^{3t} - 1$ 時、

$$\sum_{0 < z \leqslant M}{}' (d(z))^t = O(M(\log M)^{-\sigma_2}),$$

---

* *Труды Математического института, Тбилиси*, III, 1937, 1–34, 35–61.

此處 $\sum'$ 表示一和，其中之 z 都適合下面的不等式

$$(\log M)^{\sigma_2} \leqslant c_3 (d(z))^t .$$

證：由引理 2·5，我們得到

$$(\log M)^{2\sigma_2} \sum_{0<z\leqslant M}' (d(z))^t \ll \sum_{0<z\leqslant M} (d(z))^{3t} \ll$$

$$\ll M (\log M)^{2^{3t}-1} \ll M (\log M)^{\sigma_2} .$$

由此卽得出本引理.

引 理 6·2. 命 l 是一正整數（$\leqslant L^{\sigma_3}$），Q 是一 $\ll L^{\sigma_4}$ 的正整數，

$$f(x) = \frac{h}{q} x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k, \qquad (h, q) = 1,$$

此處 α 是實數. 並設 $L^{\sigma} < q \leqslant P^k L^{-\sigma}$. 則當

$$\sigma \geqslant 2^k (\sigma_0 + \sigma_3) + 2k \sigma_4 + 2^{3(k-2)}$$

時，

$$S = \sum_{\substack{lx\leqslant P \\ lx\equiv t \pmod{Q}}} e(f(lx)) = O(P_1 L^{-\sigma_0}),$$

此處 $P_1 = P/Ql$.

證：如果相合式 $lx \equiv t \pmod{Q}$ 沒有解答，則本引理不證自明．命 t' 是這相合式的最小正數解，則其他的解可以表成 $x = t' + Q y/(l, Q)$ 的形式，而 $0 \leqslant y \leqslant P_2 = P(Q, l)/Ql$. 所以 S 可以寫成

$$S = \sum_{y\leqslant P_2} f(l' y + l t'), \qquad l' = lQ/(Q, l) .$$

若 $k=1$，這引理可由引理 1·8 得出，

$$|S| = \left| \sum_{x\leqslant P_2} e\left(\frac{h}{q} (l' x + l t')\right) \right| \leqslant q \leqslant P L^{-\sigma} \leqslant P L^{-\sigma_0} .$$

假定 $k>1$. 由引理 3·3, 3·4 及 1·8 可知

$$|S|^{2^{k-1}} \ll P_2^{2^{k-1}-1}+P_2^{2^{k-1}-k}\sum_{\xi_1=1}^{P_0}\cdots\sum_{\xi_{k-1}=1}^{P_3}\min\left(P_2,\frac{1}{2\left\{P^k Q^k k!\frac{h}{q}\xi_1\cdots\xi_{k-1}\right\}}\right), \quad (1)$$

或寫成

$$|S|^{2^{k-1}} \ll P_2^{2^{k-1}-1}+P_2^{2^{k-1}-k}\sum,$$

此 $\sum$ 代表前式右邊之和.

命

$$z=P^k Q^k k!\,\xi_1\cdots\xi_{k-1}, \quad (2)$$

則得 $z\leqslant P^k Q^k k!\ P_2^{k-1}=M$.

對一固定的 z, (2) 式的解數 $\leqslant d^{k-2}(z)$. 由引理 6·1, 當 $\sigma_2\geqslant 2^{3(k-2)}-1$ 時

$$\sum \ll P_2\sum_{z=1}^{M}{}' d^{k-2}(z)+L^{\sigma_2}\sum_{z=1}^{M}\min\left(P_2,\frac{1}{2\{hz/q\}}\right)\ll$$

$$\ll M L^{-\sigma_2}P_2+L^{\sigma_2}\sum_{z=1}^{M}\min\left(P_2,\frac{1}{2\{hz/q\}}\right).$$

(由於 $\log M\gg\log P$). 由引理 3·5 及 $M P_2\ll P^k Q^k P_2^k=P^k\ll P_1^k L^{k(\sigma_3+\sigma_4)}$, 可得

$$\sum \ll M L^{-\sigma_2}P_2+L^{\sigma_2}\left(\frac{M}{q}+1\right)(P_2+q\log q)\ll$$

$$\ll P_1^k\left(L^{k(\sigma_3+\sigma_4)-\sigma_2}+L^{\sigma_2+k(\sigma_3+\sigma_4)-\sigma+1}\right).$$

取

$$\sigma_2=2^{k-1}(\sigma_0+\sigma_3)+k\sigma_4+2^{3(k-2)}-1,$$

則由 $\sigma\geqslant 2^k(\sigma_0+\sigma_3)+2k\sigma_4+2^{3(k-2)}$

可知

$$\sum \ll P_1^k L^{-2^{k-1}\sigma_0-(2^{k-1}-k)\sigma_3}.$$

代入 (1) 式,得

$$|S|^{2^{k-1}} \ll P_2^{2^{k-1}-k} P_1^k L^{-2^{k-1}\sigma_0-(2^{k-1}-k)\sigma_3} \ll P_1^{2^{k-1}} L^{-2^{k-1}\sigma_0},$$

即

$$S \ll P_1 L^{-\sigma_0}.$$

引理 6·3. 命 l 是一正整數 ($\leqslant L^{\sigma_3}$), 並命

$$\Omega = \sum_d \sum_m e(f(l\,d\,m)), \quad f(x) = \frac{h}{q}x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k,$$

此處 $(h, q)=1$, 諸 α 都是實數, $L^\sigma < q \leqslant P^k L^{-\sigma}$. Ω 中之 d 經過一適合次之條件的正整數組

$$D < d \leqslant D', \quad 1 < D < \frac{P}{l} = P_1, \quad D' \leqslant 2D.$$

又對一固定的 d, m 經過一適合次之不等式的正整數組

$$P'/d < m \leqslant P_1/d,$$

此處 P' 是一正數. 如是則當 $L^{\sigma_5} < D < P L^{-\sigma_6}$ 時,並在條件

$$\sigma_5 \geqslant 2^{2k}\sigma_0, \quad \sigma_6 \geqslant (2k+1)\sigma_3 + 2^{2k+1}\sigma_0 + 2^{3(2k-1)}$$

及

$$\sigma \geqslant 2k\sigma_3 + 2^{2k+1}\sigma_0 + 2^{3(2k-1)}$$

之下, 我們有

$$\Omega \ll P_1 L^{-\sigma_0}.$$

證：1）為簡單起見，命 $P_0=[P_1/D]$．用 Cauchy 不等式，可知

$$|\Omega|^2 \leqslant D\sum_d \left|\sum_m e\left(f(l\,d\,m)\right)\right|^2 =$$

$$= D\sum_x \sum_m \sum_{m_1} e\left(\frac{h}{q}\, l^k x^k (m^k - m_1^k) + \cdots\right), \tag{1}$$

此處 x 經過所有適合 $D < x \leqslant D'$ 的整數．對一個固定的 x, m 及 m_1 都經過某一適合不等式

$$\frac{P'}{x} < m \leqslant \frac{P_1}{x}$$

的整數組．

變換 (1) 中和號的次序，則得

$$|\Omega|^2 \leqslant D\sum_{m_1} \sum_m \sum_x e\left(\frac{h}{q}\, l^k x^k (m^k - m_1^k) + \cdots\right), \tag{2}$$

此處 m 及 m_1 經過某一適合於

$$0 < m \leqslant P_0, \qquad 0 < m_1 \leqslant P_0$$

的整數列，而對已固定的 m 及 m_1, x 經過所有適合於

$$\max\left(D,\ \frac{P'}{m},\ \frac{P'}{m_1}\right) < x \leqslant \min\left(D',\ \frac{P_1}{m},\ \frac{P_1}{m_1}\right)$$

的整數．

2）寫

$$\left|\sum_m \sum_x e\left(\frac{h}{q}\, l^k x^k (m^k - m_1^k) + \cdots\right)\right| \leqslant \sum_y^{P_0} S_y, \tag{3}$$

此處

$$S_y = \left| \sum_x e\left(\frac{h}{q} l^k x^k (y^k - m_1^k) + \cdots\right) \right|,$$

其中 x 經過在下列隔間中所有的整數:

$$\max\left(D'', \frac{P'}{y}\right) < x \leqslant \min\left(D''', \frac{P_1}{y}\right),$$

而

$$D'' = \max\left(D, \frac{P'}{m_1}\right), \qquad D''' = \min\left(D', \frac{P_1}{m_1}\right).$$

應用引理 3·3 及 3·4 可得

$$|S_y|^{2^k} = \left| \sum_x e\left(\frac{h}{q} l^k x^k (y^k - m_1^k) + \cdots\right) \right|^{2^k} \ll$$

$$\ll D^{2^k-k-1} \sum_{\xi_1}^{D} \cdots \sum_{\xi_k}^{D} \sum_x^{D} e\left(\frac{h}{q} l^k (y^k - m_1^k) k! \xi_1 \cdots \xi_k\right).$$

對 y 求和,並變換和號可得

$$\sum_y |S_y|^{2^k} \ll D^{2^k-k} \sum_{\xi_1}^{D} \cdots \sum_{\xi_k}^{D} \left| \sum_y^{P_0} e\left(\frac{h}{q} l^k (y^k - m_1^k) k! \xi_1 \cdots \xi_k\right) \right|. \qquad (4)$$

3) 若 $k=1$, 則

$$\sum_y |S_y|^2 \ll D \sum_{\xi_1}^{D} \left| \sum_y^{P_0} e\left(\frac{h}{q} l y \xi_1\right) \right| \leqslant$$

$$\leqslant D \sum_{\xi_1}^{D} \min\left(P_0, \frac{1}{\{h l \xi_1/q\}}\right) \leqslant D \sum_{\xi}^{Dl} \min\left(P_0, \frac{1}{\{h \xi / q\}}\right) \leqslant$$

$$\leqslant D\left(\frac{Dl}{q} + 1\right)(P_0 + q \log q).$$

由 (2) 式及 Cauchy 不等式

$$|\Omega|^2 \leqslant D P_0 \max_{m_1} \sum_{y}^{P_0} |S_y| \ll D P_0 \max_{m_1} \sqrt{P_0 \sum_{y}^{P_0} |S_y|^2} \leqslant$$

$$\leqslant D^2 P_0^2 \left(\left(\frac{l}{q} + \frac{1}{D}\right) \left(1 + \frac{q \log q}{P_0}\right) \right)^{1/2},$$

卽得

$$\Omega \ll D P_0 \left(\frac{l}{q} + \frac{1}{D} + \frac{l \log q}{P_0} + \frac{q \log q}{D P_0} \right)^{1/4} \ll$$

$$\ll P_1 (L^{\sigma_3 - \sigma} + L^{-\sigma_5} + L^{2\sigma_3 - \sigma_6 + 1} + L^{\sigma_3 - \sigma + 1})^{1/4} \ll P_1 L^{-\sigma_0}.$$

此處用了

$$\sigma \geqslant \sigma_3 + 1 + 4\sigma_0, \quad \sigma_5 \geqslant 4\sigma_0, \quad \sigma_6 \geqslant 2\sigma_3 + 1 + 4\sigma_0.$$

4) 假定 $k>1$. 用 Hölder 不等式，得

$$\left(\sum_{\xi_1}^{D} \cdots \sum_{\xi_k}^{D} \left| \sum_{y}^{P_0} e\left(\frac{h}{q} l^k y^k k! \xi_1 \cdots \xi_k\right) \right| \right)^{2^{k-1}} \ll$$

$$\ll D^{k(2^{k-1}-1)} \sum_{\xi_1}^{D} \cdots \sum_{\xi_k}^{D} \left| \sum_{y}^{P_0} e\left(\frac{h}{q} l^k y^k k! \xi_1 \cdots \xi_k\right) \right|^{2^{k-1}}. \tag{5}$$

由引理 3·3, 3·4 及 1·8, 可知

$$\left| \sum_{y}^{P_0} e\left(\frac{h}{q} l^k y^k k! \xi_1 \cdots \xi_k\right) \right|^{2^{k-1}} \ll$$

$$\ll P_0^{2^{k-1}-k} \sum_{\eta_1}^{P_0} \cdots \sum_{\eta_{k-1}}^{P_0} \min\left(P_0, \frac{1}{2\left\{\frac{h}{q} l^k k!^2 \xi_1 \cdots \xi_k \eta_1 \cdots \eta_{k-1}\right\}}\right), \tag{6}$$

因此，由 (5) 及 (6) 得

$$\left(\sum_{\xi_1} \cdots \sum_{\xi_k} \left| \sum_{y} e\left(\frac{h}{q} l^k y^k k! \xi_1 \cdots \xi_k\right) \right| \right)^{2^{k-1}} \ll D^{k(2^{k-1}-1)} P_0^{2^{k-1}-k} \times$$

$$\times \sum_{\xi_1}^{D} \cdots \sum_{\xi_k}^{D} \sum_{\eta_1}^{P_0} \cdots \sum_{\eta_{k-1}}^{P_0} \min\left(P_0, \frac{1}{2\left\{\frac{h}{q} l^k (k!)^2 \xi_1 \cdots \xi_k \eta_1 \cdots \eta_{k-1}\right\}}\right). \quad (7)$$

5）此和中適合

$$\xi_1 \cdots \xi_k \eta_1 \cdots \eta_{k-1} = 0$$

的諸項之和是

$$\ll D^{k 2^{k-1}} P_0^{2^{k-1}}\left(\frac{1}{D} + \frac{1}{P_0}\right) \ll D^{k 2^{k-1}} P_0^{2^{k-1}} (L^{-\sigma_5} + L^{\sigma_8 - \sigma_6}).$$

又適合

$$z = l^k k!^2 \xi_1 \cdots \xi_k \eta_1 \cdots \eta_{k-1}$$

的項數 $\leqslant (d(z))^{2k-1}$，且 $|z| \leqslant l^k k!^2 D^k P_0^{k-1}$．定義 $l^k k!^2 D^k P_0^{k-1} = M$，依照 (7)，(8) 及引理 6·1，如果 $\sigma_2 > 2^{3(2k-1)} - 1$，則得

$$\left(\sum_{\xi_1} \cdots \sum_{\xi_k} \left| \sum_{y} e\left(\frac{h}{q} l^k y^k k! \xi_1 \cdots \xi_k\right) \right|\right)^{2^{k-1}} \ll D^{k 2^{k-1}} P_0^{2^{k-1}} (L^{-\sigma_5} + L^{\sigma_8 - \sigma_6}) +$$

$$+ D^{k 2^{k-1} - k} P_0^{2^{k-1} - k}\left(M L^{-\sigma_2} P_0 + L^{\sigma_2} \sum_{0 < z \leqslant M} \min\left(P_0, \frac{1}{2\{h z/q\}}\right)\right). \quad (9)$$

由引理 3·5 及 $M \ll L^{k\sigma_3} D^k P_0^{k-1}$，可得

$$\sum_{0 < z \leqslant M} \min\left(P_0, \frac{1}{2\{h z/q\}}\right) \ll \left(\frac{M}{q} + 1\right)(P_0 + q \log q) \ll$$

$$\ll D^k P_0^k (L^{1 + k\sigma_3 - \sigma} + L^{(k+1)\sigma_3 - \sigma_6 + 1}).$$

代入 (9) 式，立得

$$\left(\sum_{\xi_1} \cdots \sum_{\xi_k} \left| \sum_{y} e\left(\frac{h}{q} l^k k! \xi_1 \cdots \xi_k (y^k - m_1^k)\right) \right|\right)^{2^{k-1}} \ll$$

$$\ll D^{k2^{k-1}} P_0^{2^{k-1}} \left(L^{-\sigma_5} + L^{k\sigma_3-\sigma_2} + L^{\sigma_2+1+k\sigma_3-\sigma} + L^{\sigma_2+(k+1)\sigma_3-\sigma_6+1}\right).$$

6) 取

$$\sigma_2 = k\sigma_3 + 2^{2k}\sigma_0 + 2^{3(2k-1)} - 1.$$

由於

$$\sigma_5 \geqslant 2^{2k}\sigma_0,\ \sigma_6 \geqslant (2k+1)\sigma_3 + 2^{2k+1}\sigma_0 + 2^{3(2k-1)}$$

及

$$\sigma > 2k\sigma_3 + 2^{2k+1}\sigma_0 + 2^{3(2k-1)},$$

可得

$$\sum_{\xi_1}\cdots\sum_{\xi_k}\left|\sum_y e\left(\frac{h}{q} l^k k!\xi_1\cdots\xi_k(y^k - m_1^k)\right)\right| \ll D^k P_0 L^{-2^{k+1}\sigma_0}.$$

由 (4) 得

$$\sum_y |S_y|^{2^k} \ll D^{2^k} P_0 L^{-2^{k+1}\sigma_0}.$$

用 Hölder 不等式，得出

$$\sum_y |S_y| \leqslant P_0^{1-2^{-k}}\left(\sum_y |S_y|^{2^k}\right)^{2^{-k}} \ll D P_0 L^{-2\sigma_0}.$$

再由 (2) 式得出

$$|\Omega|^2 \leqslant D P_0 D P_0 L^{-2\sigma_0}$$

及

$$\Omega \ll D P_0 L^{-\sigma_0} \ll P_1 L^{-\sigma_0}.$$

§3. 定理的證明

1) 以 H 代表所有不大於 $\sqrt{P}$ 的素數的乘積．以 (d) 表 H 的除數所成的數集．運用一習知的論證法，可知

$$S=\sum_{d\leqslant P}\mu(d)\,S_d+O(\sqrt{P}),$$

此處 $\mu(d)$ 是 Möbius 函數而

$$S_d=\sum_{\substack{dm\leqslant P\\ dm\equiv t\,(\bmod Q)}}e(f(dm)).$$

2) 今先估計

$$S_0=\sum_{d\leqslant L^{\lambda_1}}\mu(d)\,S_d,\qquad \lambda_1=2^{2k}(\sigma_0+\sigma_1+1),$$

的值. 在引理 6·2 中取 $l=d$, $\sigma_3=\lambda_1$, $\sigma_4=\sigma_1$ 及 σ_0+1 代替 σ_0, 則得

$$|S_d|\ll\frac{P}{Q\,d}\,L^{-\sigma_0-1}.$$

(此處用了 $\sigma\geqslant 2\,k\,\sigma_1+2^k\,(\sigma_0+1+\lambda_1)+2^{3(k-2)}$). 故

$$S_0\ll\sum_{d\leqslant L^{\lambda_1}}\frac{P}{Q\,d}\,L^{-\sigma_0-1}\ll P\,Q^{-1}\,L^{-\sigma_0}.$$

3) 以 (d_0) 表 (d) 中有偶數個素因子的數所成的數集, 而 (d_1) 表其餘部份. 命

$$S'=\sum_{L^{\lambda_1}<(d)\leqslant P}\mu(d)\,S_d=T_0-T_1,$$

此處

$$T_0=\sum_{L^{\lambda_1}<(d_0)\leqslant P}S_d,\qquad T_1=\sum_{L^{\lambda_1}<(d_1)\leqslant P}S_d.$$

今僅研究 T_0, 因爲 T_1 可以由同法得出相似的結果.

4) 討論 T_0 的一部份

$$T_0' = \sum_{L^{\lambda_1} \leqslant (d_0) \leqslant PL^{-\lambda_2}} S_d, \qquad \lambda_2 = 2^{2k+1}(\sigma_0 + \sigma_1 + 1) + 2^{3(2k-1)}.$$

將此和分爲 $O(L)$ 份,每一分和的形式如

$$D < d < D', \qquad D' \leqslant 2D.$$

以 Ω 代表其中之一. 如此則

$$\Omega = \sum_d \sum_m e(f(dm)),$$

此處 d 經過某一適合於

$$D < d \leqslant D', \qquad D' \leqslant 2D, \qquad L^{\lambda_1} \leqslant d \leqslant PL^{-\lambda_2}$$

的數列. 對已定的 d, m 經過適合於

$$0 < m < \frac{P}{d}, \qquad md \equiv t \pmod{Q}$$

的數列.

在引理 6·3 中取 $l = 1$, $\sigma_3 = 0$, $\sigma_5 = \lambda_1$, $\sigma_6 = \lambda_2$ 及以 $\sigma_0 + \sigma_2 + 1$ 代 σ_0, 則由 $\sigma \geqslant 2^{2k+1}(\sigma_0 + \sigma_1 + 1) + 2^{3(2k-1)}$, 可得

$$\Omega \ll PL^{-\sigma_0 - 1 - \sigma_1}.$$

由是卽得

$$T_0' \ll L|\Omega| \ll \frac{P}{Q} L^{-\sigma_0}.$$

5) 所留待討論之部份可以寫成

$$T_0'' = \sum_d \sum_m e(f(dm)),$$

此處 d 經過 (d_0) 中適合

$$P L^{-\lambda_3} < d \leqslant P$$

的整數，且對一固定的 d, m 經過適合

$$0 < m \leqslant P/d, \qquad m\,d \equiv \lambda \pmod Q$$

的整數． 換和號，則得

$$T_0'' = \sum_m T(m), \qquad T(m) = \sum_d e(f(d\,m)),$$

此處 m 經過整數

$$m = 1, 2, \cdots, [L^{\lambda_3}],$$

而對一固定的 m, d 則經過適合於

$$P L^{-\lambda_3} < d \leqslant \frac{P}{m}$$

的整數．

6） 以 (d_0') 表 (d_0) 之分集，其中整數有素因子 $\geqslant L^{\lambda_3}$ 者 $(\lambda_3 = \sigma_0 + \lambda_2 + \sigma_1)$；而 (d_0'') 表其餘部份． 則

$$T(m) = T'(m) + T''(m), \qquad T'(m) = \sum_{(d_0')}, \qquad T''(m) = \sum_{(d_0'')}.$$

(d_0'') 中適合於 $PL^{-\lambda_3} < d \leqslant \frac{P}{m}$ 的元素的個數小於適合以下條件的整數 l 的個數 F：(i) l 無大於一的平方因子，(ii) l 適合不等式

$$P^{1/2} < l < P,$$

(iii) l 的素因子不大於 L^{λ_3}． 假定 l 有 s 個素因子，則

$$L^{s\lambda_3} \geqslant l > P^{1/2},$$

由此得出 $s \geqslant \frac{1}{2} L/(\lambda_3 \log L)$． 又

$$d(l) = 2^s > 2^{\frac{1}{2}L/(\lambda_3 \log L)} \gg L^{\lambda_3+1}.$$

由引理 2·5,

$$F L^{\lambda_3+1} \leqslant \sum_{l=1}^{P} d(l) \ll P L,$$

卽

$$F \ll P L^{-\lambda_3}.$$

故得

$$T(m) = T'(m) + O(P L^{-\lambda_3}) = T'(m) + O\left(\frac{P}{Q} L^{-\sigma_0-\lambda_2}\right).$$

(此處用了 $\lambda_3 = \sigma_0 + \lambda_2 + 1$).

7) 以 $T_s(m)$ 表一和,其 d 經過 (d_0') 的一分集,其中元素恰有 s 個素因子 $\geqslant L^{\lambda_3}$. 由於

$$L^{\lambda_3 s} \leqslant P, \qquad s \leqslant \frac{L}{\lambda_3 \log L} < L,$$

故得

$$T'(m) = \sum_{s<L} T_s(m),$$

而

$$T_s(m) = \sum_d e(f(md))$$

乃一和,其中所經過的 d, 適合於不等式

$$P L^{-\lambda_2} < d \leqslant P_1 = \frac{P}{m},$$

且 d 乃 (d_0') 之一員,並恰有 s 個素因子 $\geqslant L^{\lambda_3}$.

8) 因爲要估計,我們引進一和

$$T_{s0}(m) = \sum_u \sum_v e(f(muv)),$$

此處 u 經過所有 $\geqslant L^{\lambda_3}$ 的素數且在 (d) 中，對已與的 u, v 經過所有適合不等式

$$\frac{PL^{-\lambda_2}}{u} < v \leqslant \frac{P_1}{u}, \quad m\,u\,v \equiv t \pmod{Q}$$

的整數，且 v 在 (d_1) 中，並恰有 $s-1$ 個素因子 $\geqslant L^{\lambda_3}$.

在 $T_s(m)$ 中每一項 $e(f(m\,d))$ 在 $T_{s0}(m)$ 中出現 s 次. 舍此而外，$T_{s0}(m)$ 中不在 $T_s(m)$ 中出現的項的形式如

$$e(f(m\,p^2\,v_1)), \quad \frac{P\,L^{-\lambda_2}}{p^2} < v_1 \leqslant \frac{P_1}{p^2},$$

此處 $p \geqslant L^{\lambda_3}$, 而 v_1 經過 (d_0)中之元素，且 v_1 恰有 $s-2$ 個素因子 $\geqslant L^{\lambda_3}$. (當 $s=1$, 則此類項不存在). 如此的項在 $T_{s0}(m)$ 出現的次數僅一次且唯一次(因為 v_1 無平方因子). 對一已與之 p, 共有 $\ll P_1/p^2$ 項. 所以

$$T_{s0}(m) = s\,T_s(m) + O\left(\sum_{L^{\lambda_3}\leqslant p} \frac{P_1}{p^2}\right) = s\,T_s(m) + O\left(\frac{P}{m}\,L^{-\lambda_3}\right).$$

故

$$T_s(m) = \frac{1}{s}\,T_{s0}(m) + O\left(\frac{P}{m\,s}\,L^{-\lambda_3}\right).$$

9) 把引理 6·3 用到 $T_{s0}(m)$ 上. 和

$$T_{s0}(m) = \sum_u \sum_v e(f(m\,u\,v))$$

中 u 乃經過 $L^{\lambda_3} \leqslant u \leqslant \sqrt{P}$ 間所有的素數. 對一固定的 u, 變數 v 經過 (d_1) 中所有適合以下諸條件的元素:

(i) v 恰有 $s-1$ 個素因子 $\geqslant L^{\lambda_3}$,

(ii) $P\,L^{-\lambda_2}/u < v \leqslant P_1/u$,

(iii) $muv \equiv t \mod Q$.

把 $L^{\lambda_3} \leqslant u \leqslant \sqrt{P}$ 分成 $O(L)$ 份,使其每一份皆可以應用引理 6·3. 今於引理 6·3 中取 $l = m$, $\sigma_3 = \lambda_2$, $\sigma_5 = \lambda_3$, 並取 σ_6 爲一任意大之整數. 且用 $\sigma_1 + \sigma_0 + 2$ 代替 σ_0. 如是則由

$$\lambda_3 \geqslant 2^{2k}(\sigma_1 + \sigma_0 + 2), \qquad \sigma \geqslant 2k\lambda_2 + 2^{2k+1}(\sigma_1 + \sigma_0 + 2) + 2^{3(2k-1)}$$

可得

$$T_{s0}(m) \ll \frac{P}{m} L^{-\sigma_0-\sigma_1-2} L = \frac{P}{m} L^{-\sigma_0-\sigma_1-1}.$$

因此得到

$$T_s(m) \ll \frac{P}{s\,m} L^{-\sigma_0-\sigma_1-1} + \frac{P}{s\,m} L^{-\lambda_3} \ll \frac{P}{s\,m} L^{-\sigma_0-\sigma_1-1},$$

此處用上了 $\lambda_3 \geqslant \sigma_0 + \sigma_1 + 1$.

最後,

$$T_0 = T_0' + T_0'' = T_0' + \sum_m T(m) \ll T_0' + \sum_m T'(m) + \sum_m \frac{P}{Q} L^{-\sigma_0-\lambda_2} \ll$$

$$\ll \frac{P}{Q} L^{-\sigma_0} + \sum_m \sum_{s<L} T_s(m) \ll \frac{P}{Q} L^{-\sigma_0} + \sum_m \sum_{s<L} \frac{P}{Q\,s\,m} L^{-\sigma_0-1} \ll$$

$$\ll \frac{P}{Q} L^{-\sigma_0}.$$

由此得到

$$S \ll \frac{P}{Q} L^{-\sigma_0}.$$

第　七　章

華林-古特拔黑問題的解數的漸近式

§ 1.

命 $f(x)$ 表一 k 次的整值多項式，其最高係數 A 是正數．並假定無整數 q (>1) 存在使對所有的 x 恆有 $f(x)\equiv f(0) \pmod q$．以 $I(N)$ 表方程

$$f(p_1)+\cdots+f(p_s)=N$$

的解答數，其中未知數 $p_1,\cdots,p_s$ 是素數．（爲簡單計，這一問題稱爲華林-古特拔黑問題）．本章之目的在證明下之定理：

定理 11. 若

$$s\geqslant\begin{cases}2^k+1 & \text{當 } 1\leqslant k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2{,}5) & \text{當 } k>10,\end{cases}$$

則

$$\left|I(N)-A^{-sa}\mathfrak{S}(N)\frac{\Gamma^s(a)}{\Gamma(sa)}\frac{N^{sa-1}}{(\log N)^s}\right|\leqslant\frac{c\,(k,s,f\text{ 的係數})\,N^{sa-1}}{(\log N)^{s+1}}\log\log N,$$

此處

$$\mathfrak{S}(N)=\sum_{q=1}^{\infty}B_s(N,q),$$

$$B_s(N,q)=\sum_{\substack{h=1\\(h,q)=1}}^{\bar q}\left(\frac{W_{h,q}}{\varphi(\bar q)}\right)^s e_q(-hN),$$

$$W_{h,q}=\sum_{\substack{l=1\\(l,q)=1}}^{\bar q}e_q(hf(l)),\quad \bar q=q(d,q),$$

此處 d 乃 $f(x)$ 的係數之最小公分母.

在證明定理 11 時我們需要一重要引理: 命 $r_{2t}(P)$ 表方程

$$f(x_1)+\cdots+f(x_t)=f(y_1)+\cdots+f(y_t),\quad 0\leqslant x,y\leqslant P,$$

的整數解答 $x_1,\cdots,x_t,y_1,\cdots,y_t$ 的組數. 則當 $k\geqslant 11$,

$$2t>k^2(2\log k+\log\log k+2{,}5)-2$$

時,

$$r_{2t}=\int_0^1|T(\alpha)|^{2t}d\alpha\ll P^{2t-k},\quad T(\alpha)=\sum_{x=1}^{P}e(f(x)\alpha).$$

§2. 若 干 引 理

引 理 7·1. 命 $\tau\geqslant 1$. 對任一實數 α 有二整數 h 及 q 存在,使

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau},\quad 0<q<\tau,\quad (h,q)=1.$$

證: 並不失去普遍性,我們可以假定 $\alpha>0$. 把 α 展開成連分數,且命

$$\frac{P_1}{Q_1}=\frac{[\alpha]}{1},\ \frac{P_2}{Q_2},\ \frac{P_3}{Q_3},\cdots$$

表它的漸近分數. 數列 Q_v 或有止境,或趨向無窮. 若止於 P_s/Q_s, $Q_s\leqslant\tau$, 則 $\alpha=P_s/Q_s$, 此引理顯然眞確. 若有一 m 使

$$Q_m<\tau\leqslant Q_{m+1},$$

則

$$\left|\alpha-\frac{P_m}{Q_m}\right|\leqslant\left|\frac{P_{m+1}}{Q_{m+1}}-\frac{P_m}{Q_m}\right|=\frac{1}{Q_mQ_{m+1}}\leqslant\frac{1}{Q_m\tau},$$

卽得本引理,其中 $h=P_m$, $q=Q_m$.

引理 7·2. (Euler 求和式). 命

$$b_1(x) = x - \lfloor x \rfloor + \frac{1}{2}.$$

用歸納法定義次之函數:

$$b_l(x+1) = b_l(x), \tag{1}$$

$$\int_0^x b_l(y)\,dy = b_{l+1}(x) - b_{l+1}(0). \tag{2}$$

命 $b > a$. 在隔間 $a \leqslant x \leqslant b$ 中,設 $g(x)$ 是一具有多次導數的函數, 其次數視我們的需要而定. 則對所有的 t

$$\sum_{\substack{m \\ a \leqslant m+t < b}} g(m+t) = \int_a^b g(x)\,dx +$$

$$+ \sum_{r=0}^{l-1} \left(g^{(r)}(b)\, b_{r+1}(t-b) - g^{(r)}(a)\, b_{r+1}(t-a)\right) - \int_a^b g^{(l)}(x)\, b_l(t-x)\,dx. \tag{3}$$

證: 1) 簡化引理:

1·1) 我們不妨假定 $t = 0$. 因為我們取 $a - t = A$, $b - t = B$, $g(x+t) = G(x)$, 則有

$$\sum_{A \leqslant m < B} G(m) = \int_A^B G(x)\,dx +$$

$$+ \sum_{r=0}^{l-1} \left(G^{(r)}(B)\, b_{r+1}(-B) - G^{(r)}(A)\, b_{r+1}(-A)\right) - \int_A^B G^{(l)}(x)\, b_l(-x)\,dx.$$

1·2) 因為上式的每邊都是可加的,所以祇須證明

$$w \leqslant A < B \leqslant w+1$$

時的情況即可,此處 w 是任一整數.

1·3) 如 1.1) 所論,我們可以假定 $w = 0$ 而不失其普徧性.

2) 當 $l=1$ 時,引理眞實. 卽

$$G(0)=\int_0^B G(x)\,dx+G(B)\,b_1(-B)-G(0)\,b_1(0)-$$

$$-\int_0^B G'(x)\,b_1(-x)\,dx \qquad \text{當 } A=0, \tag{4}$$

及

$$0=\int_A^B G(x)\,dx+G(B)\,b_1(-B)-G(A)\,b_1(-A)-$$

$$-\int_A^B G'(x)\,b_1(-x)\,dx \qquad \text{當 } 0<A<B\leqslant 1. \tag{5}$$

此二式的證明如下:

$$\int_A^B G'(x)\,b_1(-x)\,dx=\int_A^B G'(x)\left(-x-[-1]-\frac{1}{2}\right)dx=$$

$$=\left[\left(-x+\frac{1}{2}\right)G(x)\right]_A^B+\int_A^B G(x)\,dx=$$

$$=\int_A^B G(x)\,dx+\left(-B+\frac{1}{2}\right)G(B)-\left(-A+\frac{1}{2}\right)G(A)=$$

$$=\int_A^B G(x)\,dx+b_1(-B)\,G(B)-$$

$$-b_1(-A)\,G(A)-\begin{cases}0 & \text{若 } A\neq 0,\\ G(A) & \text{若 } A=0,\end{cases}$$

由於 $\frac{1}{2}=-\frac{1}{2}+1=b_l(0)+1$.

3) 歸納法. 運用分部積分法,可得

$$\int_A^B G^{(l)}(x)\,b_l(t-x)\,dx=G^{(l)}(B)\,b_{l+1}(t-B)-G^{(l)}(A)\,b_{l+1}(t-A)+$$

$$+\int_A^B G^{(l+1)}(x)\,b_{l+1}(t-x)\,dx.$$

引理已經證明.

引理 7·3. 在任一有限的隔間中 $b_l(x)$ 是一囿變函數.

證: 當 $l=1$ 時,在 $(0,1)$ 中 $b_1(x)$ 是二單調函數之差,因之,它是囿變函數. 對於一般的情况,可由 $b_l(x)$ 是 $b_{l-1}(x)$ 的積分這一性質得出.

引理 7·4. 若 $x \neq [x]$, 則

$$b_1(x)=x-[x]-\frac{1}{2}=-\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin 2\pi n x}{n}.$$

證: 祇須討論 $0<x<1$ 時的情况即可. 因

$$\log(1-z)=-\left(z+\frac{z^2}{2}+\cdots+\frac{z^n}{n}+\cdots\right),$$

故 $\frac{1}{2\pi i}\log(1-e^{2\pi i x})$ 的級數的實數部份等於引理中之右邊,而 $\frac{1}{2\pi i}\log(1-e^{2\pi i x})$ 的實數部份等於

$$\frac{1}{\pi}\operatorname{arc\,tg}\frac{\sin 2\pi x}{1-\cos 2\pi x}=x-\frac{1}{2}.$$

引理卽已證明.

引理 7·5. 命 $b>a$. 假定 $\varphi(x)$ 和 $f(x)$ 是隔間 (a,b) 中連續的實函數,在此隔間中僅有有限個* 極大值和極小值. 則

1) $$\int_a^b \varphi(x)e(x)\,dx \ll \max_{0\leqslant\xi\leqslant 1}\ \max_{a\leqslant v\leqslant b-\xi}\int_v^{v+\xi}|\varphi(x)|\,dx. \tag{6}$$

2) 假定 $f(x)$ 可求微分且適合 $|f'(x)|\leqslant\frac{1}{2}$. 則

$$\sum_{a\leqslant x\leqslant b}e^{2\pi i f(x)}-\int_a^b e^{2\pi i f(x)}\,dx \ll 1. \tag{7}$$

證: 1) 當 $b-a\leqslant 1$ 時,本引理 1) 顯然眞實.

現在假定 $a<b-1$. 如能證明

*所謂有限個極大值和極小值,乃指其個數不超過一個僅與 k 相關的數.

$$\int_a^b \varphi(x)e(x)dx \ll \max_{a\leqslant v\leqslant b-1}\int_v^{v+1} |\varphi(x)|dx, \tag{8}$$

則引理已經證明．我們也可以假定 $\varphi(x)$ 是單調的，而不失其普徧性．如若不然，我們可以分此隔間成爲有限段，每一段中 $\varphi(x)$ 是單調的．由於方法相同，我們僅討論 $\varphi(x)$ 是遞減時的情況．因爲

$$\left|\int_a^b \varphi(x)\,e(x)\,dx\right| \leqslant \int_a^{[a]+1} |\varphi(x)|\,dx + \left|\int_{[a]+1}^{[b]} \varphi(x)\,e(x)\,dx\right| + \int_{[b]}^b |\varphi(x)|\,dx,$$

所以我們祇須證明 (8) 式當 a 及 b 都是整數的情形卽可．

我們現在有

$$\begin{aligned}\int_a^b \varphi(x)\sin 2\pi x\,dx &= \int_a^{a+\frac{1}{2}} \varphi(x)\sin 2\pi x\,dx + \int_{a+\frac{1}{2}}^{a+1} \varphi(x)\sin 2\pi x\,dx + \cdots\\ &= \int_0^{\frac{1}{2}}\Big(\varphi(x+a) - \varphi(x+a+\tfrac{1}{2}) + \varphi(x+a+1) - \cdots\\ &\quad - \varphi(x+b-\tfrac{1}{2})\Big)\sin 2\pi x\,dx.\end{aligned}$$

因爲 $\varphi(x)$ 是遞減函數，所以

$$0\leqslant\varphi(x+a)-\varphi(x+a+\tfrac{1}{2})+\varphi(x+a+1)-\cdots-\varphi(x+b-\tfrac{1}{2})\leqslant\varphi(x+a).$$

由此立得

$$\begin{aligned}0 &\leqslant \int_a^b \varphi(x)\sin 2\pi x\,dx \leqslant \int_0^{\frac{1}{2}} \varphi(x+a)\sin 2\pi x\,dx \leqslant\\ &\leqslant \int_0^{\frac{1}{2}} |\varphi(x+a)|\,dx \leqslant \int_a^{a+\frac{1}{2}} |\varphi(x)|\,dx.\end{aligned}$$

用同樣方法來討論

$$\int_a^b \varphi(x)\cos 2\pi x\,dx,$$

並將所得的結果合併，卽得出本引理 1)．

2) 如 1) 的論點我們仍可以假定 $f(x)$ 是單調的. 現估計積分

$$\int_a^b f'(x)\, e^{2\pi i(f(x)\pm mx)}\, dx, \qquad m \text{ 是整數.}$$

命 $f(x) \pm mx = y$，則此積分等於

$$\int \frac{f'(x)}{f'(x) \pm m} \cdot e^{2\pi i y}\, dy.$$

由 1) 可以算出

$$\left| \int_a^b f'(x)\, e^{2\pi i(f(x)\pm mx)}\, dx \right| \leqslant \int \left| \frac{f'(x)}{m \pm f'(x)} \right| dy \ll \frac{1}{m}.$$

由此立刻有

$$\int_a^b e^{2\pi i f(x)} f'(x) \sin 2\pi m x\, dx = O\left(\frac{1}{m}\right).$$

由引理 7·4 可得

$$\left| \int_a^b e^{2\pi i f(x)} f'(x)\, b_1(-x)\, dx \right| = \frac{1}{\pi} \left| \int_a^b e^{2\pi i f(x)} f'(x) \sum_{m=1}^{\infty} \frac{\sin 2\pi mx}{m}\, dx \right| =$$

$$= \frac{1}{\pi} \left| \sum_{m=1}^{\infty} \frac{1}{m} \int_a^b e^{2\pi i f(x)} f'(x) \sin 2\pi mx\, dx \right| =$$

$$= O\left(\sum_{m=1}^{\infty} \frac{1}{m^2}\right) = O(1).$$

(逐項求積分時,運用了 $b(-x)$ 的級數是囿收斂這一點).

最後,由 Euler 的求和公式即可得出我們的引理.

引理 7·6. 命 $\Psi_1(x) = e^{x^k}$. 則

$$\Psi_1^{(r)}(x) = e^{x^k} F_r(x),$$

此處 $F_r(x)$ 是一 $(k-1)r$ 次的多項式.

此引理的證明用歸納法不難得出.

引 理 7·7. 命 $\Psi(x)=e(\beta A(qx)^k)$. 若 $q\leqslant c_1(k)\ P^{1-\epsilon}$, $|\beta|\leqslant$ $\leqslant c_2(k)\ q^{-1}\ P^{-k+1-\epsilon}$ 及 $0\leqslant x\leqslant P/q$, 則

$$|\Psi^{(r)}(x)|\leqslant c_3(A,\epsilon,r,k)\,P^{-r\epsilon}.$$

證: 由

$$|\beta|^a q\leqslant (c_2(k))^a q^{1-a} P^{-1+a-\epsilon a}\leqslant$$
$$\leqslant (c_2(k))^a (c_1(k))^{1-a} P^{(1-\epsilon)(1-a)-1+a-\epsilon a}$$

及

$$(|\beta|^a q)^k x^{k-1}\leqslant|\beta|\,q^k\left(\frac{P}{q}\right)^{k-1}\leqslant c_2(k)\,P^{-\epsilon},$$

由引理 7·6, 可知

$$|\Psi^{(r)}(x)|=|\Psi(x)\,F_r((2\pi\beta A)^a q x)((2\pi i\beta A)^a q)^r|\leqslant$$
$$\leqslant c_4(A,\epsilon,r,k)\,(1+(|\beta|^a q x)^{(k-1)r})\,(|\beta|^a q)^r\leqslant$$
$$\leqslant c_3(A,\epsilon,r,k)\,P^{-r\epsilon}.$$

引 理 7·8. 命 $f(x)=A_k x^k+\cdots+A_1 x+A_0$,

$$\Phi(x)=e(\beta f(qx)).$$

則在引理 7·7 的條件下

$$|\Phi^{(r)}(x)|\leqslant c_5(A_k,\cdots,A_0,\epsilon,r,k)\,P^{-r\epsilon}.$$

證: 當 $k=1$ 時引理顯然成立. 命

$$\Phi(x)=\Psi(x)\,\Phi_1(x),\qquad \Phi_1(x)=e(\beta f(qx)-\beta A_k(qx)^k).$$

假定此引理對 $k-1$ 時眞實. 卽當 $|\beta|\ll q^{-1}\ P^{-k+2-\epsilon}$ 時

$$|\Phi_1^{(r)}(x)|\leqslant c_6(A_{k-1},\cdots,A_0,\epsilon,r,k)\,P^{-r\epsilon}.$$

由於 $q^{-1}P^{-k+2-\varepsilon} > q^{-1}P^{-k+1-\varepsilon}$，則當 $|\beta| \leqslant q^{-1}P^{-k+1-\varepsilon}$ 時

$$|\Phi_1^{(r)}(x)| \leqslant c_6 P^{-r\varepsilon}.$$

故由

$$\Phi^{(r)}(x) = \Psi^{(r)}(x)\Phi_1(x) + \binom{r}{1}\Psi^{(r-1)}(x)\Phi_1'(x) + \cdots + \Psi(x)\Phi_1^{(r)}(x)$$

可得出

$$|\Phi^{(r)}(x)| \leqslant c_5 P^{-r\varepsilon}.$$

§3. Farey 分割

對隔間 $-\frac{1}{\tau} \leqslant \alpha \leqslant 1-\frac{1}{\tau}$ 中任一數 α，由引理 7·1 已知有一對整數 h 及 q 使

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q\tau}, \quad 0 < q < \tau, \quad (h, q) = 1,$$

此處 $\tau = P^{k r 1+\varepsilon}$.

在隔間 $\left(-\frac{1}{\tau}, 1-\frac{1}{\tau}\right)$ 中任一有理點 $\frac{h}{q}$ 附近做一分隔間

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q\tau}.$$

對 $q \leqslant P^{1-\varepsilon}$ 的分隔間用 $\mathfrak{M}(h,q)$ 表之；隔間 $\left(-\frac{1}{\tau}, 1-\frac{1}{\tau}\right)$ 中之點不在任一分隔間 $\mathfrak{M}(h,q)$ 之中者以 E 表之.

今證任二 $\mathfrak{M}(h,q)$ 都無公共之點. 若不然，設

$$\alpha = \frac{h}{q} + \beta, \quad \alpha_1 = \frac{h_1}{q_1} + \beta_1, \quad |\beta| \leqslant \frac{1}{q\tau}, \quad |\beta_1| \leqslant \frac{1}{q_1\tau},$$

則

$$\left|\frac{h_1}{q_1} - \frac{h}{q}\right| = |\beta_1 - \beta|, \text{ 即 } \frac{1}{qq_1} \leqslant \frac{1}{q\tau} + \frac{1}{q_1\tau}, \quad 1 \leqslant \frac{q_1+q}{\tau}.$$

由於 $q + q_1 \leqslant 2P^{1-\epsilon}$，故此爲不可能.

因此，命

$$T(\alpha) = \sum_{x=1}^{P} e(f(x)\alpha),$$

則當 P 充分大時有

$$I_{2t}(P) = \int_0^1 |T(\alpha)|^{2t} d\alpha = \int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}} |T(\alpha)|^{2t} d\alpha =$$

$$= \int_E |T(\alpha)|^{2t} d\alpha + \sum_{q \leqslant P^{1-\varepsilon}} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \int_{\mathfrak{M}(h,q)} |T(\alpha)|^{2t} d\alpha.$$

§4. 估計展在 E 上的積分的絕對值

引理 7·9. 當 $k > 10$ 及 $t > k^2(2\log k + \log\log k + 2{,}5) - 2$ 時，

$$\int_E |T(\alpha)|^{2t} d\alpha \ll P^{2t-k}.$$

證：由定理 8 及 9，命 $t = t_1 + t_2$，可得

$$\int_E |T(\alpha)|^{2t} d\alpha \ll P^{2(1-1/\sigma_k)t_2 + 2t_1 - k + \delta + \varepsilon}$$

$$\ll P^{2t - k + \delta - 2t_2/\sigma_k + \varepsilon}.$$

今取 $t_2 = 2k^2$，及

$$l = \left[\frac{\log\left(\frac{1}{2}k(k+1)\log k^2\right)}{-\log(1-a)} + 1\right].$$

如此則

$$\delta = \frac{1}{2} k(k+1)(1-a)^l < \frac{1}{2\log k},$$

而

$$\frac{2t_2}{\sigma_k} > \frac{4k^2}{2k^2(2\log k + \log\log k + 3)} > \frac{1}{2\log k}.$$

因此,如能證明

$$t_1 + t_2 < k^2 (2 \log k + \log\log k + 2{,}5) - 4,$$

則立刻得出本引理.

由

$$l \leqslant \frac{\log\left(\frac{1}{2} k (k+1) \log k^2\right)}{-\log(1-a)} + 1 \leqslant \left(1 - \frac{a}{2}\right) k \log(k^2 \log k) + 2 \leqslant$$

$$\leqslant k \log(k^2 \log k) - \log k - \frac{1}{2} \log\log k + 2,$$

可知

$$t_1 + t_2 \leqslant \frac{1}{4}(k^2 + k + 2) + lk + 2k^2 \leqslant$$

$$\leqslant k^2 (2 \log k + \log\log k + 2{,}5) - 2.$$

因此證明了本引理.

§5. 關於 $\mathfrak{W}(h, q)$ 的引理

命

$$T^*(\alpha, h, q) = \bar{q}^{-1} S_{h,q} \int_0^P e(f(y)\beta)\, dy,$$

此處

$$S_{h,q} = \sum_{v=1}^{\bar{q}} c_q(hf(v)), \quad \bar{q} = q(q, d),$$

此處 d 乃 $f(x)$ 的係數的最小公分母.

引理 7·10.

$$T^*(\alpha, h, q) \ll q^{-a+\varepsilon} \min(P, |\beta|^{-a}).$$

證:由定理 1 (推理 1·2) 已知

$$S_{h,q} \ll q^{1-a+\varepsilon}.$$

又因為 $\int_0^P e(\beta f(y))dy=O(P)$，所以我們所待證明的是下面的結論：當 $|\beta|^{-a}\leqslant P$ 時，

$$\int_0^P e(\beta f(y))\,dy \ll |\beta|^{-a}.$$

存在一常數 c 使

$$f(y+c)=g(y)$$

是一正係數的多項式．如此則

$$\int_c^P e(\beta f(y))\,dy=\int_0^{P-c} e(\beta g(y))\,dy.$$

命 $w=|\beta|\,g(y)$．則 y 可以看成是 w 的遞增函數．命 $w_0=|\beta|g(0)$．則由第二中值定理可知

$$\int_{w_0}\frac{e^{\pm 2\pi i w}}{|\beta|\,g'(y)}\,dw \ll \left(\frac{1}{|\beta|\,g'(y)}\right)_{w=w_0} \ll \frac{1}{|\beta|^a}.$$

引理 7·11. 命 $\alpha=\frac{h}{q}+\beta$．當 $q\leqslant P^{1-\varepsilon}$ 及 $|\beta|\leqslant q^{-1}P^{-k+1-\varepsilon}$ 時，

$$T(\alpha)-T^*(\alpha,h,q)\ll q^{1-a+\varepsilon}.$$

證：我們有

$$T(\alpha)=\sum_{x=0}^{P} e(f(x)\alpha)=$$

$$=\sum_{v=1}^{q}\sum_{\substack{0\leqslant r<P\\ r\equiv v\,(\mathrm{mod}\,q)}} e\left(\frac{h}{q}f(r)\right)e(\beta f(r))=$$

$$=\sum_{v=1}^{q} e\left(\frac{h}{q}f(v)\right)\Lambda_v,$$

此處

$$\Lambda_v = \sum_{\substack{j \\ 0 \leqslant \bar{q} j + v \leqslant P}} e(\beta f(\bar{q} j + v)) = \sum_{\substack{j \\ 0 \leqslant j + \frac{v}{q} < \frac{P}{q}}} \Phi\left(j + \frac{v}{q}\right),$$

及

$$\Phi(x) = e(\beta f(\bar{q} x)).$$

運用引理 7·2，得

$$\Lambda_v = \int_0^{P/\bar{q}} \Phi(x)\, dx + \sum_{r=1}^{l-1} \left(\Phi^{(r)}\left(\frac{P}{\bar{q}}\right) b_{r+1}\left(\frac{v}{\bar{q}} - \frac{P}{\bar{q}}\right) - \Phi^{(r)}(0)\, b_{r+1}\left(\frac{v}{\bar{q}}\right)\right) -$$

$$- \int_0^{P/\bar{q}} \Phi^{(l)}(x)\, b_l\left(\frac{v}{\bar{q}} - x\right) dx.$$

由

$$\int_0^{P/\bar{q}} \Phi(x)\, dx = \int_0^{P/\bar{q}} e(\beta f(\bar{q} x))\, dx = \frac{1}{\bar{q}} \int_0^P e(\beta f(y))\, dy,$$

可知

$$T(\alpha) = T^*(a, h, q) + \sum_{r=1}^{l-1} \left(\Phi^{(r)}\left(\frac{P}{\bar{q}}\right) a_{r+1}\left(\frac{P}{\bar{q}}\right) - \Phi^{(r)}(0)\, a_{r+1}(0)\right) - R,$$

此處

$$a_{r+1}(t) = \sum_{v=1}^{\bar{q}} e_q(h f(v))\, b_{r+1}\left(\frac{v}{\bar{q}} - t\right)$$

及

$$R = \sum_{v=1}^{q} e_q(h f(v)) \int_0^{P/\bar{q}} \Phi^{(l)}(x)\, b_l\left(\frac{v}{\bar{q}} - x\right) dx.$$

現在取 $l = \left[\frac{1}{\varepsilon}\right] + 1$，則由引理 7·8，可知

$$\Phi^{(l)}(x) \ll P^{-1},$$

及

$$R \ll \bar{q} \int_0^{P/\bar{q}} P^{-1}\, dx \ll 1.$$

命

$$s_v = \sum_{x=1}^{v} e_q(hf(x)).$$

$$a_{r+1}(t) = s_1 b_{r+1}\left(\frac{1}{q} - t\right) + \sum_{v=2}^{q} (s_v - s_{v-1})\, b_{r+1}\left(\frac{v}{q} - t\right) =$$

$$= \sum_{m=1}^{q-1} s_m \left(b_{r+1}\left(\frac{m}{q} - t\right) - b_{r+1}\left(\frac{m+1}{q} - t\right)\right) + s_q\, b_{r+1}(1-t).$$

由定理 2,

$$s_v = O(q^{1-a+\varepsilon}).$$

因 $b_{r+1}(x)$ 是一囿變函數,故得

$$|a_{r+1}(t)| \ll q^{1-a+\varepsilon}\left(\sum_{m=1}^{q-1}\left|b_{r+1}\left(\frac{m}{q} - t\right) - b_{r+1}\left(\frac{m+1}{q} - t\right)\right| + 1\right) \ll$$

$$\ll q^{1-a+\varepsilon}.$$

再用引理 7·8 卽得

$$T(\alpha) - T^*(\alpha, h, q) \ll \left(\sum_{r=1}^{l-1} P^{-r+\varepsilon} + 1\right) q^{1-a+\varepsilon} \ll$$

$$\ll q^{1-a+\varepsilon}.$$

§6. 估計展開在 $\mathfrak{M}(h, q)$ 上的積分之數值

引 理 7·12. 當 $2t > 2k+1$ 時,

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T(\alpha)|^{2t}\, d\alpha \ll P^{2t-k}.$$

證: 由引理 7·10 及 7·11, 可知在 $\mathfrak{M}(h,q)$ 上

$$T(\alpha) \ll q^{-a+\varepsilon} \min(P, |\beta|^{-a}) + q^{1-a+\varepsilon} \ll$$

$$\ll q^{-a+\varepsilon} \min(P, |\beta|^{-a}).$$

引理中所述及的和不超過

$$\ll \sum_{\mathfrak{M}} \int_{\mathfrak{M}} q^{-2ta+\varepsilon} \min(P^{2t}, |\beta|^{-2ta})\, d\beta \ll$$

$$\ll \sum_{q \leqslant P^{1-\varepsilon}} \sum_{h=1}^{q} q^{-2ta+\varepsilon} \left(\int_0^{P^{-k}} P^{2t}\, d\beta + \int_{P^{-k}} \beta^{-2ta}\, d\beta\right) \ll$$

$$\ll P^{2t-k} \sum_{q \leqslant P^{1-\varepsilon}} q^{1-2ta+\varepsilon} \ll P^{2t-k},$$

(由於 $\sum q^{1-2ta}$ 的收歛性).

引理 7·13. 當 $k \geqslant 14$ 及

$$t > k^2 (2 \log k + \log\log k + 2{,}5) - 2$$

時,

$$I_{2t}(P) \ll P^{2t-k}.$$

這是由引理 7·9 及 7·12 直接推出的結果.

§7. 證明定理所必需的引理

命 $N = f(P)$,

$$\mathfrak{T}(\alpha) = \sum_{p \leqslant P} e(f(p)\alpha),$$

$$\mathfrak{T}^*(\alpha, h, q) = \frac{1}{A^a} \frac{W_{h,q}}{\varphi(q)} \sum_{2 \leqslant n \leqslant f(p)} \frac{e(n\beta)}{n^{1-a} \log n},$$

此處 A 是 $f(x)$ 的最高方次的係數, $W_{h,q}$ 的定義見本章之首.

我們仍如 §3 來分割隔間 $-\frac{1}{\tau} \leqslant \alpha \leqslant 1 - \frac{1}{\tau}$, 但現在却用 $q \leqslant \tau = NL^{-\sigma}$. 此處我們選擇了 σ 使定理 10 中的 σ_0 大於定理 4 中的 $c_2(k, k)$ 加上某一整數 s_1.

用 $\mathfrak{M}(h,q)$ 代表隔間

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau},\qquad q\leqslant L^{\sigma}.$$

用 E 代表隔間 $\left(-\frac{1}{\tau},1-\frac{1}{\tau}\right)$ 中所有不在 $\mathfrak{M}(h,q)$ 內的點．容易證明(如前)所有的 $\mathfrak{M}(h,q)$ 無公共點．

引理 7·14 (Siegel—Walfisz)*．假定 $q\leqslant L^{\sigma}$, $(l,q)=1$, $N\leqslant P$．命 $\pi(n;l,q)$ 代表算術級數 $l+qx$ 中不大於 n 的素數的個數．則

$$\pi(n;l,q)=\frac{1}{\varphi(q)}\operatorname{li}n+O\left(Pe^{-c_1\sqrt{L}}\right),$$

此處 $\operatorname{li}x=\int_2^x\frac{dt}{\log t}$，符號 O 所包含的常數與 q 無關．

引理 7·15. 在 $\mathfrak{M}(h,q)$ 上，

$$\mathfrak{T}(\alpha)-\mathfrak{T}^*(\alpha,h,q)=O\left(Pe^{-c_2\sqrt{L}}\right).$$

證：命 $\alpha=\frac{h}{q}+\beta$．又命

$$S_n=\sum_{f(p)\leqslant n}e_q(hf(p)),\quad n\leqslant N.$$

則

$$S_n=\sum_{\substack{l=1\\(l,\bar q)=1}}^{\bar q}e_q(hf(l))\,\pi(n';l,\bar q)+O(q^{\epsilon}),$$

此處 n' 是方程 $f(x)=n$ 的最大正根．(當 n 充分大時，n' 是一定存在的，且是唯一的)．今往證明

*Math. Zs., **40** (1936), 592—601, Hilfsatz 3. 關於完整的證明，可參考：Н. Г. Чудаков, введение в теорию L-функций дирихле, 或 T. Estermann, Introduction to modern prime number theory.

$$n' - \left(\frac{n}{A}\right)^a \ll 1.$$

這是由於：

$$n' - \left(\frac{n}{A}\right)^a = n' - \left(\frac{f(n')}{A}\right)^a = n' - (n'^k + O(n'^{k-1}))^a =$$

$$= n'(1 - (1 + O(n'^{-1}))^a) = O(1).$$

由引理 7·14，對充分大的 n 我們有

$$\pi(n'; l, \bar{q}) = \frac{1}{\varphi(\bar{q})} \mathrm{li}\, n' + O(P e^{-c_1\sqrt{L}}) =$$

$$= \frac{1}{\varphi(\bar{q})} \mathrm{li}\left(\frac{n}{A}\right)^a + O(P e^{-c_1\sqrt{L}}).$$

最後的等式對所有的不大於 P 的數 n' 都眞實．由此得出

$$S_n = \sum_{\substack{l=1 \\ (l,q)=1}}^{\bar{q}} e_q(hf(l)) \left(\frac{1}{\varphi(\bar{q})} \mathrm{li}\left(\frac{n}{A}\right)^a + O(P e^{-c_1\sqrt{L}})\right) + O(q^\varepsilon) =$$

$$= \sum_{\substack{l=1 \\ (l,\bar{q})=1}}^{\bar{q}} \frac{e_q(hf(l))}{\varphi(\bar{q})} \mathrm{li}\left(\frac{n}{A}\right)^a + O(P e^{-c_3\sqrt{L}}) =$$

$$= \frac{W_{h,q}}{\varphi(\bar{q})} \mathrm{li}\left(\frac{n}{A}\right)^a + O(P e^{-c_3\sqrt{L}}).$$

因此

$$\mathfrak{T}(\alpha) = \sum_{n=2}^{N} (S_n - S_{n-1}) e(n\beta) + O(1) =$$

$$= \sum_{n=2}^{N} S_n (e(n\beta) - e((n+1)\beta)) + S_N e((N+1)\beta) + O(1) =$$

$$= \frac{W_{h,q}}{\varphi(\bar{q})} \left(\sum_{n=2}^{N} \mathrm{li}\left(\frac{n}{A}\right)^a (e(n\beta) - e((n+1)\beta)) + \mathrm{li}\left(\frac{N}{A}\right)^a e((N+1)\beta)\right) +$$

$$+ O(P e^{-c_4\sqrt{L}}).$$

由於

$$\mathrm{li}\left(\frac{n}{A}\right)^a-\mathrm{li}\left(\frac{n-1}{A}\right)^a=\int_{((n-1)/A)^a}^{(n/A)^a}\frac{dt}{\log t}=$$

$$=A^{-a}\int_{(n-1)^a}^{n^a}\frac{dy}{\log(yA^{-a})}=\frac{1}{A^a n^{1-a}\log n}+O\left(\frac{1}{n^{2-a}\log n}\right),$$

因而得出所需要的結果.

引理 7·16. 當 $|\beta|\leqslant\frac{1}{2}$ 時,

$$\mathfrak{T}^*(\alpha,h,q)\ll q^{-a+\varepsilon}\min(P,|\beta|^{-a}).$$

在 $\mathfrak{M}(h,q)$ 上對於 $\mathfrak{T}(\alpha)$ 也有類似的結果.

證: 由定理 1 的推理 1·3 可得

$$\mathfrak{T}^*(\alpha,h,q)\ll q^{-a+\varepsilon}\sum_{n\leqslant f(P)}\frac{1}{n^{1-a}}\ll$$

$$\ll q^{-a+\varepsilon}P.$$

(此處用了 $\varphi(q)\geqslant\frac{q}{d(q)}\gg q^{1-\varepsilon}$). 又

$$\sum_{n\leqslant N}\frac{e(n\beta)}{n^{1-a}\log n}=\sum_{n\leqslant|\beta|^{-1}}\frac{e(n\beta)}{n^{1-a}\log n}+\sum_{N\geqslant n>|\beta|^{-1}}\frac{e(n\beta)}{n^{1-a}\log n}.$$

以 $\sum_1$ 及 $\sum_2$ 分別表示這兩個和. 顯然有

$$\left|\sum\nolimits_1\right|\leqslant\sum_{n\leqslant|\beta|^{-1}}\frac{1}{n^{1-a}\log n}=O(|\beta|^{-a}).$$

命 $S_n=\sum_{|\beta|^{-1}<m<n}e(m\beta)$,由分部求和法可得

$$\left|\sum\nolimits_2\right|=\left|\sum_{N\geqslant n>|\beta|^{-1}}\frac{e(n\beta)}{n^{1-a}\log n}\right|=\left|\sum_{N\geqslant n>|\beta|^{-1}}\frac{S_n-S_{n-1}}{n^{1-a}\log n}\right|\leqslant$$

$$\leqslant \sum_{N \geqslant n > |\beta|^{-1}} |S_n| \left(\frac{1}{n^{1-a}\log n} - \frac{1}{(n+1)^{1-a}\log(n+1)} \right).$$

因爲 $|S_n| \leqslant \frac{1}{\beta}$，可知

$$\left|\sum\nolimits_2\right| \leqslant \sum_{n > |\beta|^{-1}} \frac{1}{\beta} \left(\frac{1}{n^{1-a}\log n} - \frac{1}{(n+1)^{1-a}\log(n+1)} \right) \ll |\beta|^{-c}.$$

這證明了引理中的第一個結論.

由引理 7·15，可知

$$\mathfrak{T}(\alpha) = \mathfrak{T}^*(\alpha, h, q) + O(P e^{-c_2\sqrt{L}}).$$

因爲 $Pe^{-c_2\sqrt{L}} \ll Pq^{-a}$ 及 $Pe^{-c_2\sqrt{L}} \ll |\beta|^{-a} q^{-a}$，可得

$$\mathfrak{T}(\alpha) \ll q^{-a+\epsilon} \min(P, |\beta|^{-a}).$$

§8. 定理的證明

我們先證明一個與定理 11 略有不同的定理.

定理 11′. 假定

$$s \geqslant \begin{cases} 2^k + 1 & \text{當 } 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2{,}5) & \text{當 } k > 10. \end{cases}$$

則對任一已給的整數 s_1，常有

$$\left| I_s(N) - A^{-sa}\mathfrak{S}(N)\Psi(N) \right| \leqslant \frac{c(k, s_1, f(x)\text{ 的係數})\, N^{sa-1}}{(\log N)^{s_1}},$$

此處

$$\Psi(N) = \sum_{\substack{n_1+\cdots+n_s=N \\ n_\nu \geqslant 2}} \frac{1}{n_1^{1-a}\log n_1 \cdots n_s^{1-a}\log n_s}.$$

證：1） 我們有

$$I_s(N)=\int_0^1 \mathfrak{T}^s(\alpha)\,e(-N\alpha)\,d\alpha=\int_{\frac{1}{\tau}}^{1-\frac{1}{\tau}} \mathfrak{T}^s(\alpha)\,e(-N\alpha)\,d\alpha=$$

$$=\int_E \mathfrak{T}^s(\alpha)\,e(-N\alpha)\,d\alpha+\sum_{\mathfrak{M}(h,q)}\int_{\mathfrak{M}(h,q)} \mathfrak{T}^s(\alpha)\,e(-N\alpha)\,d\alpha.$$

2） 當 $k>10$，由於 $s>2k^2(2\log k+\log\log k+2{,}5)$，我們可以選擇整數 t，使

$$s-2t\geqslant 1,\quad t>k^2(2\log k+\log\log k+2{,}5)-2.$$

由定理 10 及引理 7·13，可得

$$\int_E \mathfrak{T}^s(\alpha)\,e(-N\alpha)\,d\alpha \ll (P\,L^{-\sigma_0})^{s-2t}\int_0^1 |\,\mathfrak{T}(\alpha)\,|^{2t}\,d\alpha \ll$$

$$\ll P^{s-2t}\,L^{-s_1}\int_0^1 |\,T(\alpha)\,|^{2t}\,d\alpha \ll$$

$$\ll P^{s-k}\,L^{-s_1}.$$

當 $1\leqslant k\leqslant 10$ 時，由定理 4 可得

$$\int_E (\mathfrak{T}(\alpha))^{2^k+1}\,e(-N\alpha)\,d\alpha \ll P\,L^{-s_1-c_2(k,k)}\int_0^1 |\,T(\alpha)\,|^{2^k}\,d\alpha \ll$$

$$\ll P^{2^k-k+1}\,L^{-s_1}$$

（由於 σ 的選擇）.

3） 由引理 7·15，7·16 及簡單的不等式

$$|\,\xi^s-\eta^s\,|\leqslant s\,|\,\xi-\eta\,|\max(|\,\xi\,|^{s-1},|\,\eta\,|^{s-1}),$$

在 $\mathfrak{M}(h,q)$ 上我們有下面的結果：

$$|\mathfrak{T}^s(\alpha)-\mathfrak{T}^{*s}(\alpha,h,q)|\leqslant s|\mathfrak{T}(\alpha)-\mathfrak{T}^*(\alpha,h,q)|\max(|\mathfrak{T}(\alpha)|^{s-1},|\mathfrak{T}^*(\alpha,h,q)|^{s-1})\ll$$

$$\ll P\,e^{-c_2\sqrt{L}}\,(q^{-\alpha+\varepsilon})^{s-1}\min(P,|\,\beta\,|^{-\alpha})^{s-1}.$$

在 $\mathfrak{M}(h,q)$ 上求積分，即得

$$\int_{\mathfrak{M}(h,q)} \mathfrak{T}^s(\alpha)\, e(-N\alpha)\, d\alpha - \int_{\mathfrak{M}(h,q)} \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\alpha \ll$$

$$\ll P e^{-c_2\sqrt{L}}\, q^{-a(s-1)+\varepsilon} \left(\int_0^{P^{-k}} P^{s-1}\, d\beta + \int_{P^{-k}} \beta^{-a(s-1)}\, d\beta\right) \ll$$

$$\ll q^{-a(s-1)+\varepsilon} P^{s-k} e^{-c_2\sqrt{L}}.$$

對所有的 $\mathfrak{M}(h,q)$ 求和，得出

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} \mathfrak{T}^s(\alpha)\, e(-N\alpha)\, d\alpha - \sum_{\mathfrak{M}} \int_{\mathfrak{M}} \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\alpha \ll$$

$$\ll P^{s-k} e^{-c_2\sqrt{L}} \sum_{q \leqslant L^\sigma} q^{1-a(s-1)+\varepsilon} \ll$$

$$\ll P^{s-k} e^{-c_6\sqrt{L}}.$$

4) 由引理 7·16，我們有

$$\int_{\mathfrak{M}(h,q)} \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\alpha - \int_0^1 \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\beta \ll$$

$$\ll q^{-as+\varepsilon} \int_{q^{-1}\tau^{-1}}^{\infty} \beta^{-as}\, d\beta \ll$$

$$\ll q^{-1+\varepsilon} P^{s-k} L^{-\sigma(sa-1)}.$$

故

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\alpha - \sum_{\mathfrak{M}} \int_0^1 \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\beta \ll$$

$$\ll P^{s-k} L^{-\sigma(sa-1)} \sum_{q \leqslant L^\sigma} q^\varepsilon \ll$$

$$\ll P^{s-k} L^{-\sigma(sa-2)+\varepsilon} \ll P^{s-k} L^{-s_1}.$$

(由於 $2s_1 < \sigma$ 及 $sa - 2 \geqslant \frac{1}{2}$).

5）我們有

$$\sum_{\mathfrak{M}} \int_0^1 \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\beta =$$

$$= A^{-sa} \sum_{\mathfrak{M}} \left(\frac{W_{h,q}}{\varphi(\bar{q})}\right)^s e\left(-\frac{Nh}{q}\right) \int_0^1 \left(\sum_{2 \leqslant n \leqslant N} \frac{e(n\beta)}{n^{1-a}\log n}\right)^s e(-N\beta)\, d\beta =$$

$$= A^{-sa} \sum_{q \leqslant L^\sigma} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \left(\frac{W_{h,q}}{\varphi(\bar{q})}\right)^s e\left(-\frac{Nh}{q}\right) \Psi(N),$$

此處 $\Psi(N)$ 之定義見定理 11′.

6）我們有

$$\left|\sum_{q > L^\sigma} \sum_{\substack{h=1 \\ (h,q)=1}}^{\bar{q}} \left(\frac{W_{h,q}}{\varphi(\bar{q})}\right)^s e\left(-\frac{Nh}{q}\right)\right| \leqslant \sum_{q > L^\sigma} q \cdot q^{-sa+\varepsilon} \ll L^{(2-sa)\sigma+\varepsilon} \ll L^{-s_1}.$$

故

$$\sum_{q \leqslant L^\sigma} \sum_{\substack{h=1 \\ (h,q)=1}}^{\bar{q}} \left(\frac{W_{h,q}}{\varphi(\bar{q})}\right)^s e\left(-\frac{Nh}{q}\right) = \mathfrak{S}(N) + O(L^{-s_1}).$$

7）總結 3)，4)，5）及 6）的結果，我們得出

$$\sum_{\mathfrak{M}(h,q)} \int_{\mathfrak{M}(h,q)} \mathfrak{T}^{*s}(\alpha, h, q)\, e(-N\alpha)\, d\alpha = \mathfrak{S}(N) A^{-sa} \Psi(N) + O(N^{sa-1} L^{-s_1}).$$

再由 1）及 2）的結果可知

$$I_s(N) = \mathfrak{S}(N) A^{-sa} \Psi(N) + O(N^{sa-1} L^{-s_1}).$$

§9. 定理 11 的證明

引理 7·17. 當 $0 < \lambda_1 < 1$ 及 $\lambda_2 \geqslant \lambda_1$ 時，

$$\sum_{n=1}^{N-1} \frac{1}{n^{1-\lambda_1}(N-n)^{1-\lambda_2}} = \frac{\Gamma(\lambda_1)\Gamma(\lambda_2)}{\Gamma(\lambda_1+\lambda_2)} N^{\lambda_1+\lambda_2-1}(1 + O(N^{-\lambda_1})).$$

證：寫

$$\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{1-\lambda_2}}=N^{\lambda_1+\lambda_2-1}\sum_{n=1}^{N-1}\frac{\frac{1}{N}}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}.$$

對 $\frac{n}{N}\leqslant x\leqslant\frac{n+1}{N}$，命 $x=\frac{n}{N}+\frac{\theta}{N}(0\leqslant\theta\leqslant 1)$，則得

$$\frac{1}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}-\frac{1}{x^{1-\lambda_1}(1-x)^{1-\lambda_2}}=$$

$$=\frac{1}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}\left(1-\left(1+\frac{\theta}{n}\right)^{\lambda_1-1}\left(1-\frac{\theta}{N-n}\right)^{\lambda_2-1}\right)=$$

$$=\frac{1}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}\left(O\left(\frac{1}{n}\right)+O\left(\frac{1}{N-n}\right)\right).$$

因此

$$\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{1-\lambda_2}}=N^{\lambda_1+\lambda_2-1}\left(\int_0^1 x^{\lambda_1-1}(1-x)^{\lambda_2-1}\,dx+\right.$$

$$\left.+O\left(\sum_{n=1}^{N-1}\frac{\frac{1}{nN}}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}+\sum_{n=1}^{N-1}\frac{\frac{1}{(N-n)N}}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}\right)\right)=$$

$$=N^{\lambda_1+\lambda_2-1}\frac{\Gamma(\lambda_1)\Gamma(\lambda_2)}{\Gamma(\lambda_1+\lambda_2)}+O\left(\sum_{n=1}^{N-1}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}+\right.$$

$$\left.+\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{2-\lambda_2}}\right).$$

因爲

$$\sum_{n=1}^{N-1}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}=\sum_{n\leqslant\frac{1}{2}N}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}+\sum_{N>n>\frac{1}{2}N}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}\ll$$

$$\ll N^{\lambda_2-1}\sum_{n\leqslant\frac{1}{2}N}\frac{1}{n^{2-\lambda_1}}+N^{\lambda_1-2}\sum_{N>n>\frac{1}{2}N}\frac{1}{(N-n)^{1-\lambda_2}}\ll$$

$$\ll N^{\lambda_2-1}$$

及

$$\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{2-\lambda_2}}\ll N^{\lambda_1+\lambda_2-1-\min(1,\lambda_2)}\begin{cases}1 & \text{若 } \lambda_2\neq 1,\\ \log N & \text{若 } \lambda_2=1,\end{cases}$$

卽得出本引理.

引 理 7·18.

$$\sum_{\substack{n_1+\cdots+n_s=N\\ n_\nu>0}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}}=\frac{\Gamma^s(a)}{\Gamma(sa)}N^{sa-1}(1+O(N^{-a})).$$

證: 由引理 7·17 已知此引理當 $s=2$ 時眞實. 今假定引理對 $s-1$ 眞實而運用歸納法. 由引理 7·17 可知

$$\sum_{\substack{n_1+\cdots+n_s=N\\ n_\nu>0}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}}=\sum_{n_1=1}^{N-s+1}\frac{1}{n_1^{1-a}}\sum_{n_2+\cdots+n_s=N-n_1}\frac{1}{n_2^{1-a}\cdots n_s^{1-a}}=$$

$$=\sum_{n_1}\frac{1}{n_1^{1-a}}\frac{\Gamma^{s-1}(a)}{\Gamma((s-1)a)}(N-n_1)^{(s-1)a-1}+O\left(\sum_{n_1}\frac{1}{n_1^{1-a}(N-n)^{1-(s-2)a+a}}\right)=$$

$$=\frac{\Gamma^s(a)}{\Gamma(sa)}N^{sa-1}(1+O(N^{-a})).$$

引 理 7·19.

$$\sum_{\substack{n_1+\cdots+n_s=N\\ n_\nu>1}}\frac{1}{n_1^{1-a}\log n_1\cdots n_s^{1-a}\log n_s}=\frac{\Gamma^s(a)}{\Gamma(sa)}\frac{N^{sa-1}}{L^s}\left(1+O\left(\frac{\log L}{L}\right)\right).$$

證：命

$$\Psi_\mu(N)=\sum_{\substack{n_1+\cdots+n_s=N\\ n_\nu>1}}\frac{1}{n_1^{1-a}\log n_1\cdots n_\mu^{1-a}\log n_\mu\cdot n_{\mu+1}^{1-a}\cdots n_s^{1-a}},\quad 0<\mu\leqslant s.$$

則

$$\Psi_\mu(N)=\frac{1}{L}\Psi_{\mu-1}(N)+O\left(\frac{\Psi_\mu(N)\log L}{L}\right)+O\left(\frac{N^{sa-1}}{L^{s+1}}\right).\qquad(1)$$

此式的證明如下：分和爲兩部份：

$$\Psi_\mu(N)=\sum_{n_\mu\leqslant NL^{-\delta}}+\sum_{n_\mu>NL^{-\delta}}=S_1+S_2.$$

則

$$S_1\leqslant\frac{1}{(\log 2)^s}\sum_{\substack{n_1+\cdots+n_s=N\\ n_\mu\leqslant NL^{-\delta}}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}}\ll$$

$$\ll\sum_{n_\mu\leqslant NL^{-\delta}}\frac{1}{n_\mu^{1-a}}\sum_{n_1+\cdots+n_{\mu-1}+n_{\mu+1}+\cdots+n_s=N-n_\mu}\frac{1}{n_1^{1-a}\cdots n_{\mu-1}^{1-a}n_{\mu+1}^{1-a}\cdots n_s^{1-a}}\ll$$

$$\ll\sum_{n_\mu\leqslant NL^{-\delta}}\frac{1}{n_\mu^{1-a}}(N-n_\mu)^{(s-1)a-1}\ll$$

$$\ll N^{(s-1)a-1}(NL^{-\delta})^a=N^{sa-1}L^{-\delta a}\ll N^{sa-1}L^{-s-1}.$$

此處取 $\delta=k(s+1)$. 又

$$S_2=\frac{1}{L}\sum_{\substack{n_1+\cdots+n_s=N\\ n_\mu>NL^{-\delta}}}\frac{1}{n_1^{1-a}\log n_1\cdots n_{\mu-1}^{1-a}\log n_{\mu-1}\cdot n_\mu^{1-a}\cdots n_s^{1-a}}+$$

$$+\sum\frac{1}{n_1^{1-a}\log n_1\cdots n_\mu^{1-a}\cdots n_s^{1-a}}\left(\frac{1}{\log n_\mu}-\frac{1}{\log N}\right)=$$

$$= \frac{1}{L}\Psi_{\mu-1}(N) + O\left(\frac{N^{s\alpha-1}}{L^{s+1}}\right) + O\left(\frac{\log L}{L}\Psi_{\mu}(N)\right).$$

這證明了 (1) 式.

由 (1) 式可知

$$\Psi_{\mu}(N) = \frac{1}{L}\Psi_{\mu-1}(N) + O\left(\frac{\Psi_{\mu-1}(N)\log L}{L^2}\right) + O\left(\frac{N^{s\alpha-1}}{L^{s+1}}\right).$$

續用多次可以推得

$$\Psi_s(N) = \frac{1}{L^s}\Psi_0(N) + O\left(\frac{\Psi_0(N)\log L}{L^{s+1}}\right) + O\left(\frac{N^{s\alpha-1}}{L^{s+1}}\right) =$$

$$= \frac{1}{L^s}\Psi_0(N) + O\left(\frac{N^{s\alpha-1}}{L^{s+1}}\log L\right).$$

由引理 7·18 得出本引理.

由定理 11′ 及引理 7·19 可以得出本章開始所宣稱的定理 (定理 11).

第　八　章

奇　異　級　數

§1.

今研究 $f(x)=x^k$ 時奇異級數的性質.

命 $p^\theta \| k$,

$$\gamma=\begin{cases}\theta+2 & 若\ p=2,\ 2|k,\\ \theta+1 & 其他的情况,\end{cases}$$

及

$$K=\prod_{(p-1)|k} p^\gamma.$$

定理 12. 假定 $s\geqslant 3k+1$ 及對所有適合 $(p-1)|k$ 的 p, 常有 $s\equiv N \pmod{p^\gamma}$. 並取 $f(x)=x^k$. 則 $\mathfrak{S}(N)\geqslant A>0$, 此處 A 並不依於 N.

§2. 關於三角和的引理

引理 8·1. 若 $(q_1,q_2)=1$, 則

$$W_{h,q_1q_2}=W_{hq_1^{k-1},q_2}W_{hq_2^{k-1},q_1}$$

及

$$B_s(N,q_1q_2)=B_s(N,q_1)B_s(N,q_2).$$

證: 命 $l=l_1q_2+l_2q_1$, 則

$$W_{h,q_1q_2}=\sum_{\substack{l_1=1\\(l_1,q_1)=1}}^{q_1}\sum_{\substack{l_2=1\\(l_2,q_2)=1}}^{q_2}e_{q_1q_2}(hq_2^kl_1^k+hq_1^kl_2^k)=W_{hq_2^{k-1},q_1}W_{hq_1^{k-1},q_2}.$$

又命 $h = h_1 q_2 + h_2 q_1$，則

$$B_s(N, q_1 q_2) = \sum_{\substack{h_1=1 \\ (h_1, q_1)=1}}^{q_1} \sum_{\substack{h_2=1 \\ (h_2, q_2)=1}}^{q_2} \left(\frac{W_{h_2 q_1^k, q_2}}{\varphi(q_2)}\right)^s \left(\frac{W_{h_1 q_2^k, q_1}}{\varphi(q_1)}\right)^s e_{q_1}(-h_1 N) e_{q_2}(-h_2 N) =$$

$$= \sum_{\substack{h_1=1 \\ (h_1, q_1)=1}}^{q_1} \sum_{\substack{h_2=1 \\ (h_2, q_2)=1}}^{q_2} \left(\frac{W_{h_2, q_2}}{\varphi(q_2)}\right)^s \left(\frac{W_{h_1, q_1}}{\varphi(q_1)}\right)^s e_{q_1}(-h_1 N) e_{q_2}(-h_2 N) =$$

$$= B_s(N, q_1) B_s(N, q_2).$$

引理 8·2. 命

$$\mu \geqslant \begin{cases} 1 & \text{若 } p > 2, \\ 2 & \text{若 } p = 2. \end{cases}$$

若

$$x \equiv y + z p^{\mu} \pmod{p^{\mu+1}},$$

則

$$x^p \equiv y^p + y^{p-1} z p^{\mu+1} \pmod{p^{\mu+2}}.$$

證： 寫

$$x = y + z p^{\mu} + m p^{\mu+1}.$$

由 $3\mu > \mu + 2$，可知

$$x^p \equiv (y + z p^{\mu})^p \equiv y^p + y^{p-1} z p^{\mu+1} + \frac{1}{2}(p-1) p y^{p-2} z^2 p^{2\mu} \pmod{p^{\mu+2}}.$$

若 $p > 2$，則有

$$\frac{1}{2}(p-1) p y^{p-2} z^2 p^{2\mu} \equiv 0 \pmod{p^{\mu+2}}.$$

當 $p = 2$，由 $\mu \geqslant 2$，$2\mu \geqslant \mu + 2$，故

$$\frac{1}{2}p(p-1)y^{p-2}z^2p^{2\mu}\equiv 0 \pmod{p^{\mu+2}}.$$

從此二式可以得出本引理.

引理 8·3. 若 $t>\gamma$ 及 $p\nmid h$, 則

$$W_{h,p^t}=0.$$

證: 命 $l=l_1+l_2p^{t-\theta-1}$, 則由重複運用引理 8·2 可得

$$l^{p^\theta}\equiv l_1^{p^\theta}+l_1^{p^\theta-1}l_2p^{t-1} \pmod{p^t}.$$

於是

$$l^k\equiv l_1^k+k\,l_1^{k-1}l_2p^{t-\theta-1} \pmod{p^t}.$$

由此推得

$$W_{h,p^t}=\sum_{\substack{l_1=1\\(l_1,p)=1}}^{p^{t-\theta-1}}\sum_{l_2=0}^{p^{\theta+1}}e_{p^t}\left(h\left(l_1^k+p^{t-\theta-1}k\,l_1^{k-1}l_2\right)\right)=0.$$

(由於 $p\nmid l_1kp^{-\theta}$).

引理 8·4. 相合式

$$x^k\equiv a \pmod p,\qquad p\nmid a,$$

或無解,或有 $(k,p-1)$ 個解. 當 x 經過 $1,2,\cdots,p-1 \pmod p$ 時, x^k 經過 $(p-1)/(k,p-1)$ 個互不相合的數, mod p.

證: 相合式 $x^k\equiv 1 \pmod p$ 有 $(p-1,k)$ 個解. 此點可由 $x^{p-1}\equiv 1 \pmod p$ 推得之. 又命

$$a_1,\cdots,a_{(k,p-1)}$$

表其諸解. 若 $x_1^k\equiv a \pmod p$, 則

$$x_1a_1,\cdots,x_1a_{(k,p-1)}$$

都是 $x^k\equiv a \pmod p$ 的解，且無他解．所以相合式

$$x^k\equiv a \pmod p,\qquad p\nmid a,$$

或無解，或有 $(k, p-1)$ 個解．因之得出本引理．

引理 8·5. 若 $(h, q)=1$，則

$$|W_{h,q}|\leqslant c_1(h,\varepsilon)\,q^{1/2+\varepsilon}.$$

證：1）設 q 是一素數 p．則由引理 8·4 可知

$$\frac{1}{p}\sum_{h=1}^{p}\left|\sum_{x=1}^{p}e_p(hx^k)\right|^2=\sum_{x^k\equiv y^k \pmod p}\sum 1=(k,p-1)(p-1)+1.$$

考察和

$$\sum_{x=1}^{p}e_p(hx^k)=\sum_{x=1}^{p}e_p(h(\lambda x)^k)=\sum_{x=1}^{p}e_p(h\lambda^k x^k),\qquad \lambda=1,\cdots,p-1.$$

由於 λ^k 經過 $(p-1)/(k,p-1)$ 個互不相合的整數，mod p，故

$$\frac{p-1}{(k,p-1)}\left|\sum_{x=1}^{p}e_p(hx^k)\right|^2\leqslant\sum_{h=1}^{p}\left|\sum_{x=1}^{p}e_p(hx^k)\right|^2\leqslant$$

$$\leqslant\Big((k,p-1)(p-1)+1\Big)p.$$

因之，

$$\left|\sum_{x=1}^{p}e_p(hx^k)\right|\leqslant\sqrt{\frac{k^2p^2}{p-1}}\leqslant 2k\sqrt{p},$$

即

$$|W_{h,p}|\leqslant 2k\sqrt{p}.$$

2）若 $p|k$，由引理 8·3 易見

$$W_{h,p^l}=O(1).$$

又由引理 8·3 可見當 $p \nmid k$ 及 $t > \gamma = \theta + 1 = 1$ 時也有

$$W_{h, p^t} = O(1).$$

由 1) 可知對所有的 p 常有

$$|W_{h,p}| \leqslant 2k\sqrt{p},$$

卽當 $p \geqslant (2k)^{1/\varepsilon}$ 時,

$$|W_{h,p}| \leqslant p^{\frac{1}{2}+\varepsilon}.$$

命 $q = p_1^{l_1} \cdots p_t^{l_t}$, $p_1 < p_2 < \cdots < p_t$, 則由引理 8·1 可知

$$|W_{h,q}| = \prod_{p_i \leqslant k^{1/\varepsilon}} |W_{h_i, p^{l_i}}| \prod_{p_i > k^{1/\varepsilon}} |W_{h_i, p^{l_i}}| = O(q^{\frac{1}{2}+\varepsilon}).$$

§3. 關於相合式的引理

引理 8·6. 以 $M_s(p^t, N)$ 表相合式

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^t}, \quad p \nmid x_1 \cdots x_s, \quad 0 < x_\nu < p^t,$$

的解數. 則

$$\varphi(p^t)^{-s} p^t M_s(p^t, N) = 1 + \sum_{a=1}^{t} B_s(N, p^a).$$

證: 有

$$M_s(p^t, N) = p^{-t} \sum_{\substack{l_1=1 \\ p \nmid l_1}}^{p^t} \cdots \sum_{\substack{l_s=1 \\ p \nmid l_s}}^{p^t} \sum_{h=1}^{p^t} e_{p^t}(h(l_1^k + \cdots + l_s^k - N)) =$$

$$= p^{-t} \sum_{h=1}^{p^t} W_{h,p^t}^s e_{p^t}(-hN) = p^{-t} \varphi^s(p^t)(1 + \sum_{a=1}^{t} B_s(N, p^a)).$$

引理 8·7 (Cauchy). 命 $x_1,\cdots,x_m$ 代表 m 個不同的剩餘系 (mod p^l), 而 $y_1,\cdots,y_n$ 代表 n 個不同的剩餘系 (mod p^l), 且任意二 y 的差非 p 的倍數. 則形如 x_i+y_j $(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n)$ 所代表的不同的剩餘系 (mod p^l) 的數目不小於 $\min\ (m+n-1,\ p^l)$.

證: 今用歸納法於 n. 當 $n=1$, 此引理顯然眞實,因 x_i+y_1 $(1\leqslant i\leqslant m)$ 代表了 m 個不同的剩餘系.

命 $z_1,\cdots,z_t$ 代表形如 x_i+y_j 的不同的剩餘系, mod p^l. 不失其普遍性可以假定 $t<p^l$. 並以 X,Y,Z 分別代表集合 $x_1,\cdots,x_m$; $y_1,\cdots,y_n$; $z_1,\cdots,z_t$.

當 $n\geqslant 2$, 我們可以證明, 若 $p\nmid y$, 則 $z+y$ 不能都在 Z 中. 因爲如果不然,則對任一 λ, $z+\lambda y$ 常在 Z 中. 而 t 將等於 p^l. 所以一定有一整數 f 存在,使 $f-y$ 在 Z 中,而 f 不在 Z 中. 重新排列 y 及 z 使其適合以下的條件: 有一 r $(1\leqslant r\leqslant n)$ 存在使

$$f \text{ 不在 } Z \text{ 中};$$

$$f-y_s=z_s,\qquad \text{當 } 1\leqslant s\leqslant r;$$

$$f-y_{s'} \text{ 不在 } Z \text{ 中, 當 } r<s'\leqslant n.$$

(當 $r=n$ 時最後情況不存在).

當 $1\leqslant s<r<s'\leqslant n$ 時, $z_s-y_{s'}$ 不在 X 中,因若不然,則 $f-y_{s'}\equiv f+ +x-z_s\equiv x+y_s$ 將在 Z 中. 又當 $1\leqslant s\leqslant r$ 時, z_s 不在 X 中,因若不然,則 $f=x+y$ 將在 Z 中.

今討論由形如 x_i+y_j $(1\leqslant i\leqslant m,\ r<j\leqslant n)$ 的剩餘系所組成的數集 Z'. Z' 乃 Z 之一分集. 因 $z_1,\cdots,z_r$ 在 Z 中,而不在 Z' 中,所以 Z' 的元素的個數 $t'\leqslant t-r$.

應用歸納法假定可知 $t'\geqslant m+(n-r)$. 因之得出

$$t\geqslant t'+r\geqslant m+n-1.$$

引理 8·8. 當 $s\geqslant 3k$ 及 $(p-1)\nmid k$, 則

$$M_s(p^\gamma,N)>0.$$

證：顯然可知 $p>2$.

1）$p\nmid k$，則 $\gamma=1$. 由 $(p-1)\nmid k$ 及引理 8·4，可知 x^k 給與

$$d=\frac{p-1}{(k,p-1)}>1$$

個不同的剩餘系，mod p. 由引理 8·7，$x_1^k+\cdots+x_s^k$ $(p\nmid x_1\cdots x_s)$ 給與

$$\min(d+(d-1)(s-1),p)$$

個不同的剩餘系，mod s. 當

$$s\geqslant 2k>\frac{p-1}{\frac{1}{2}d}\geqslant\frac{p-1}{d-1}$$

時，

$$\min(d+(d-1)(s-1),p)=p.$$

2）設 $k=p^{\theta}k_0$，$p\nmid k_0$. 由於

$$x^{p^{\theta}k_0}\equiv x^{k_0}\pmod p \text{ 及 } (p-1)\nmid k_0,$$

所以 x^k 至少經過 $(p-1)/(p-1,k_0)$ (>1) 個不同的剩餘系，mod p. 故

$$x_1^k+\cdots+x_s^k,\qquad p\nmid x_1\cdots x_s,$$

給與

$$\min\left(\frac{p-1}{(p-1,k_0)}+\left(\frac{p-1}{(p-1,k_0)}-1\right)(s-1),p^{\gamma}\right)$$

個不同的剩餘系，mod p^{γ}. 由於

$$s-1\geqslant 3k-1\geqslant\frac{2pk}{p-1}-1\geqslant\frac{p^{\gamma}}{\frac{1}{2}\frac{p-1}{(k_0,p-1)}}-1\geqslant\frac{p^{\gamma}-1}{\frac{p-1}{(k_0,p-1)}-1}-1,$$

可知 $x_1^k+\cdots+x_s^k$ $(p\nmid x_1\cdots x_s)$ 給與 p^{γ} 個不同的剩餘系.

引理 8·9. 若 $s \equiv N \pmod{p^\gamma}$，則

$$M_s(p^\gamma, N) > 0.$$

此引理的證明十分明顯.

§4. 奇異級數的正性質

引理 8·10. 當 $s > 4$ 時，奇異級數 $\mathfrak{S}(N)$ 絕對收斂. 當 $k=1$，此結果可進一步改善為 $s>2$.

證：由引理 8·3 有

$$|\mathfrak{S}(N)| \leqslant \sum_{q=1}^{\infty} |B_s(N, q)| \ll \sum_{q=1}^{\infty} q^{1-\frac{1}{2}s+\varepsilon}.$$

當 $k=1$ 時，$W_{k,q} = \mu(q)$ (Möbius 函數). 而 $|\mu(q)| \leqslant 1$，故

$$|\mathfrak{S}(N)| \leqslant \sum_{q=1}^{\infty} |B_s(N, q)| \ll \sum_{q=1}^{\infty} q^{1-s}.$$

引理 8·11. 當 $s > 4$ 時，

$$\mathfrak{S}(N) = \prod_p \chi_p(N),$$

此處

$$\chi_p(N) = 1 + \sum_{t=1}^{\gamma} B_s(N, p^t).$$

當 $k=1$，此結果可以進一步改善為 $s > 2$.

證：此引理可由引理 8·1，8·3 及 8·10 直接推得.

定理的證明. 由引理 8·6，8·8 及 8·9 已知：對所有的 p，

$$\chi_p(N) > 0.$$

又

$$|B_s(N, p)| \leqslant p\left(\frac{2k\sqrt{p}}{p-1}\right)^s \leqslant (4k)^s p^{-\frac{1}{2}s+1}.$$

所以當 $p > (4k)^{4s}$ 時,

$$x_p > 1 - p^{-s/2+1+1/4}.$$

又當 $s > 4$ 時,

$$\mathfrak{S}(N) \geqslant \prod_{p \leqslant (4k)^{4s}} x_p \prod_{p > (4k)^{4s}} (1 - p^{-5/4}) \geqslant A > 0.$$

同法證明 $k = 1,\ s > 2$ 的情況.

§5. 定理 11 及 12 的推理

易於得出以下的定理: 假定 $s \geqslant s_0$, 而

$$s_0 \geqslant \begin{cases} 2^k + 1 & \text{若 } 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2{,}5) & \text{若 } k > 10. \end{cases}$$

所有的充分大的 $\equiv s \pmod K$ 的整數 N 可以表成 s 個素數的 k 次方的和.

爲了更具體起見,我們引出幾個特例:

推理 1. 所有的充分大的奇數是三素數的和.

推理 2. 所有的充分大的 $\equiv 5 \pmod{24}$ 的整數可以表成五個素數的平方之和.

推理 3. 所有的充分大的奇數可以表成九個素數的立方的和.

推理 4. 所有的充分大的 $\equiv 17 \pmod{240}$ 的整數可以表成十七個素數的四次方之和.

今引入以下的定義以結束本章. 以 $H(k)$ 表有次之性質的最小整數 s: 所有的充分大的 $\equiv s \pmod K$ 的整數可以表成 s 個素數的 k 乘方之和. 本章之結果可用下列的公式總結之:

$$H(k) \leqslant \begin{cases} 2^k + 1 & \text{若 } 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2{,}5) & \text{若 } k > 10. \end{cases}$$

第　九　章

華林－古特拔黑問題進一步的研究

§ 1.

本章的目的在證明較第八章 § 5 更好的結果：命 k 表一整數 $\geqslant 4$，$a=1/k$，

$$b=\begin{cases}2k^2(2\log k+\log\log k+3) & \text{當 } k>12,\\ 2^{k-1} & \text{當 } k\leqslant 12,\end{cases}$$

及

$$m=\left[\frac{\log\frac{1}{2}b+\log(1-2a)}{-\log(1-a)}\right].$$

定理 13. 命 $s_0=s_0(k)=2k+2m+7$ 及 $s\geqslant s_0$，則所有的充分大(卽 $\geqslant c(k)$）的相合於 $s(\bmod K)$ 的整數 N 是 s 個素數的 k 次方之和．換言之：

$$H(k)\leqslant 2k+2m+7.$$

當 k 充分大時，

$$m\sim 2k\log k$$

及

$$s_0\sim 4k\log k.$$

此結果當 $k\geqslant 5$ 時較上章 § 5 的結果爲佳．對較小的 k，卽 $k=4, 5, 6, 7$ 及 8，本章將給與更好的結果：

$$H(4)\leqslant 15,\quad H(5)\leqslant 25,\quad H(6)\leqslant 39,\quad H(7)\leqslant 55,\quad H(8)\leqslant 75.$$

§2. 與華林問題有關的引理

命 N 爲一大整數，$P = \frac{1}{2} N^a$，

$$T(\alpha, P) = \sum_{P \leqslant n \leqslant 2P} e(n^k \alpha),$$

$$T_i(\alpha) = T(\alpha, 2^{-i} P^{(1-a)^i}), \qquad i = 0, 1, \cdots, m+1.$$

$$Q(\alpha) = T_1(\alpha) \cdots T_m(\alpha) T_{m+1}^2(\alpha) =$$

$$= \sum_n r_{m+2}(n) e(n\alpha),$$

$$R(\alpha) = T_0(\alpha) Q(\alpha)$$

$$= \sum_n r_{m+3}(n) e(n\alpha),$$

$$T_0^k(\alpha) R(\alpha) = \sum_n r_{m+k+3}(n) e(n\alpha).$$

如此顯然可得

$$c_1 P^{k-1-(k-2)(1-a)^{m+1}} \leqslant Q(0) \leqslant c_2 P^{k-1-(k-2)(1-a)^{m+1}}.$$

我們的基本引理是

$$\sum_n r_{m+k+3}^2(n) = \int_0^1 |T_0^k(\alpha) R(\alpha)|^2 d\alpha = O(P^{k+2} Q^2(0)).$$

引理 9·1. 有

$$\sum_n r_{m+3}^2(n) = \int_0^1 |R(\alpha)|^2 d\alpha = O(P\, Q(0)\, L^{c_3}).$$

證：上式左邊的意義就是方程

$$x_0^k + \cdots + x_m^k + x_{m+1}^k + x'^k_{m+1} = y_0^k + \cdots + y_m^k + y_{m+1}^k + y'^k_{m+1} \tag{1}$$

適合

$$2^{-i} P^{(1-a)^i} \leqslant x_i,\ y_i \leqslant 2^{1-i} P^{(1-a)^i}$$

的整數解 x_i, y_i 的組數. 由 (1) 式可以得出,當 P 充分大時, $x_i = y_i$ ($i = 0, 1, 2, \cdots, m$). 證明此點,假定 v 是第一個使 $x_v \neq y_v$ 的足標,如此則

$$|x_v^k - y_v^k| = k \left| \int_{y_v}^{x_v} t^{k-1}\, dt \right| \geqslant k\,(P^{(1-a)^v} 2^{-v})^{k-1}.$$

此不等式右端當 P 相當大時大於

$$y_{v+1}^k + \cdots + y_{m+1}^k + y'^k_{m+1}.$$

因之, (1) 式是不可能的. 這證明了 $x_i = y_i$ ($i = 0, 1, 2, \cdots, m$). 由定理 4, 方程

$$x_{m+1}^k + x'^k_{m+1} = y_{m+1}^k + y'^k_{m+1}$$

的解數是 $O(P^{2(1-a)^{m+1}} L^{c_3})$. 引理於是乎證明了.

把隔間 $-\frac{1}{\tau} \leqslant \alpha \leqslant 1 - \frac{1}{\tau}$ 仍照第七章 §3 分開. $\mathfrak{M}(h,q)$ 及 E 都仍有原來的定義.

引理 9·2.

$$\int_E |T_0^k(\alpha) R(\alpha)|^2\, d\alpha = O(P^{k+2} Q^2(0)).$$

證: 由定理 9 已知

$$T_0(\alpha) = O(P^{1-\frac{1}{b}+\varepsilon}).$$

故

$$\int_E |T_0^{2k}(\alpha) R^2(\alpha)| \, d\alpha \ll P^{2k(1-1/b)+\varepsilon} \int_0^1 |R^2(\alpha)| \, d\alpha \ll$$

$$\ll P^{1+2k(1-1/b)+\varepsilon} Q(0) \ll$$

$$\ll P^{2k(1-1/b)+2-k+(k-2)(1-a)^{m+1}+\varepsilon} Q^2(0) \ll$$

$$\ll P^{k+2} Q^2(0).$$

注意,今用到

$$(k-2)(1-a)^{m+1} < \frac{2k}{b}.$$

引理 9·3.

$$\sum_{\mathfrak{M}(h,q)} \int_{\mathfrak{M}(h,q)} |T_0^k(\alpha) R(\alpha)|^2 \, d\alpha = O(P^{k+2} Q^2(0)).$$

證：由引理 7·12 可得

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T_0^k(\alpha) R(\alpha)|^2 \, d\alpha = \sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T_0^{2k+2}(\alpha)| \, |Q^2(\alpha)| \, d\alpha \leqslant$$

$$\leqslant Q^2(0) \sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T_0(\alpha)|^{2k+2} \, d\alpha \ll$$

$$\ll P^{k+2} Q^2(0).$$

引理 9·4.

$$\sum_n r_{k+m+3}^2(n) \ll P^{k+2} Q^2(0).$$

證：由引理 9·2 及 9·3 卽可得出.

§3. 定理 13 的證明

命

$$\mathfrak{T}(\alpha, P)=\sum_{P<p\leqslant 2P} e(p^k\alpha), \quad \mathfrak{T}_0^*(\alpha, h, q)=\frac{W_{h,q}}{\varphi(q)}\sum_{p^k<n\leqslant(2P)^k}\frac{e(n\beta)}{n^{1-a}\log n}.$$

對應地我們定義 $\mathfrak{T}_i(\alpha)$, $i=0,1,\cdots,m,m+1$, $\mathfrak{Q}(\alpha)$ 及 $\mathfrak{M}(\alpha)$. 命

$$\mathfrak{T}_0^{k+1}(\alpha)\,\mathfrak{Q}(\alpha)=\sum_n r'_{m+k+3}(n)\,e(n\alpha)$$

及

$$\mathfrak{T}^{2k+3}(\alpha)\,\mathfrak{Q}^2(\alpha)=\sum_n r'_{2m+2k+7}(n)\,e(n\alpha),$$

則 $r_{2m+2k+7}$ 乃方程

$$n=p_1^k+\cdots+p_{2m+2k+7}^k$$

的解數,其中 $p_1,\cdots,p_{2m+2k+7}$ 適合某些條件. 把隔間 $-\frac{1}{\tau}\leqslant\alpha\leqslant 1-\frac{1}{\tau}$ 如第七章 §7 分開.

引 理 9·5.

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}}|\mathfrak{T}_0^{2k+3}(\alpha)-\mathfrak{T}_0^{*2k+3}(\alpha,h,q)|\,\mathfrak{Q}^2(\alpha)\,d\alpha\ll P^{k+3}Q^2(0)\,e^{-c_4\sqrt{L}}.$$

證: 由引理 7·15 及 7·16, 在 $\mathfrak{M}(h,q)$ 上

$$\mathfrak{T}_0^{2k+3}(\alpha)-\mathfrak{T}_0^{*2k+3}(\alpha,h,q)\ll(q^{-a+\varepsilon})^{2k+2}\min(P,|\beta|^{-a})^{2k+2}\,P\,e^{-c_5\sqrt{L}},$$

因此所求的和不超過

$$\ll P^{k+3}Q^2(0)\,e^{-c_4\sqrt{L}}.$$

引 理 9·6.

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}}|\mathfrak{T}_0^{*2k+3}(\alpha,h,q)|\left|\mathfrak{Q}^2(\alpha)-A^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2m+4}\right|d\alpha\ll P^{k+3}Q^2(0)\,e^{-c_6\sqrt{L}},$$

此處

$$c_7 \frac{Q(0)}{L^{m+2}} \leqslant \Lambda \leqslant c_8 \frac{Q(0)}{L^{m+2}}.$$

證：我們有不等式

$$\left|\mathfrak{Q}(\alpha)-\mathfrak{Q}\left(\frac{h}{q}\right)\right| \leqslant \sum_n r'_{m+2}(n)\,|\,e(n\alpha)-e(nh/q)\,| \leqslant$$

$$\leqslant |\beta| \sum_n n\, r'_{m+2}(n) \ll P^{k-1}\,|\beta|\, Q(0) \ll$$

$$\ll P^{-1} L^{\sigma} Q(0).$$

再用引理 7·14,

$$\mathfrak{T}\left(\frac{h}{q}\right)=\sum_{2^{-i}P^{(1-a)^i}\leqslant p\leqslant 2^{-i+1}P^{(1-a)^i}} e_q(h p^k)=$$

$$=\sum_{\substack{l=1\\(l,q)=1}}^{q} e_q(h l^k)\left(\pi\left(2^{-i+1}P^{(1-a)^i}; l, q\right)-\pi\left(2^{-i}P^{(1-a)^i}; l, q\right)\right)+O(q^{\varepsilon})=$$

$$=\frac{W_{h,q}}{\varphi(q)}\int_{2^{-i}P^{(1-a)^i}}^{2^{-i+1}P^{(1-a)^i}} \frac{dx}{\log x}+O\left(P^{(1-a)^i} e^{-c_9\sqrt{L}}\right).$$

因此

$$\mathfrak{Q}\left(\frac{h}{q}\right)=\left(\frac{W_{h,q}}{\varphi(q)}\right)^{m+2}\Lambda+O\left(Q(0)\, e^{-c_{10}\sqrt{L}}\right),$$

此處

$$\Lambda=\left(\prod_{i+1}^{m+1}\int_{2^{-i}P^{(1-a)^i}}^{2^{-i+1}P^{(1-a)^i}}\frac{dx}{\log x}\right)\left(\int_{2^{-(m+1)}P^{(1-a)^{m+1}}}^{2^{-m}P^{(1-a)^{m+1}}}\frac{dx}{\log x}\right).$$

由於

$$\frac{x}{\log x} \ll \int_2^x \frac{dt}{\log t} \ll \frac{x}{\log x},$$

所以這一 Λ 適合於引理中的不等式.

由此得出

$$\left|\mathfrak{Q}^2(\alpha)-A^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2(m+2)}\right|\leqslant\left|\mathfrak{Q}(\alpha)-A\left(\frac{W_{h,q}}{\varphi(q)}\right)^{m+2}\right|Q(0)\ll$$

$$\ll Q^2(0)\,e^{-c_{10}\sqrt{L}}.$$

由引理 7·16 可知,所討論的和不超過

$$\ll\sum_{q\leqslant L^\sigma}q\cdot Q^2(0)\,e^{-c_{10}\sqrt{L}}\,q^{-2-3a+\varepsilon}\left(\int_0^{P^{-k}}P^{2k+3}\,d\beta+\int_{P^{-k}}\beta^{-2-3a}\,d\beta\right)$$

$$\ll P^{k+3}\,Q^2(0)\,e^{-c_6\sqrt{L}}.$$

引 理 9·7.

$$\sum_{\mathfrak{M}}\left(\int_0^1-\int_{\mathfrak{M}}\right)\left|\mathfrak{T}_0^{*2k+3}(\alpha,h,q)\,A^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2m+4}\right|d\alpha\ll P^{k+3}\,Q^2(0)\,L^{-s_1}.$$

證: 此式的左方不超過

$$\ll\sum_{q\leqslant L^\sigma}q\cdot Q^2(0)\,q^{-(2m+4)\sigma}\,q^{-(2+3a)+\varepsilon}\int_{q^{-1}N^{-1}L^\sigma}\beta^{-2-3a}\,d\beta\ll$$

$$\ll P^{k+3}\,Q^2(0)\,L^{-\sigma(1+3a)}\ll P^{k+3}\,Q^2(0)\,L^{-s_1}.$$

(由於 $s_1<\sigma$).

引 理 9·8.

$$\int_E\left|\mathfrak{T}^{2k+3}(\alpha)\,\mathfrak{Q}^2(\alpha)\right|d\alpha\ll P^{k+3}\,Q^2(0)\,L^{-s_1}.$$

證: 由定理 10 及 引理 9·4, 可知

$$\int_E\left|\mathfrak{T}^{2k+3}(\alpha)\,\mathfrak{Q}^2(\alpha)\right|d\alpha\ll P\,L^{-s_1}\int_0^1\left|T^{2k+2}(\alpha)\,Q^2(\alpha)\right|d\alpha\ll$$

$$\ll P^{k+3}\,Q^2(0)\,L^{-s_1}.$$

引理 9·9.

$$r'_{2k+2m+7}(N) = A^2 \mathfrak{S}(N) \Psi(N) + O(P^{k+3} Q^2(0) L^{-\varepsilon_1}),$$

此處

$$c_{11} P^{k+3} L^{-2k-3} < \Psi(N) < c_{12} P^{k+3} L^{-2k-3}.$$

證：由引理 9·5, 9·6, 9·7 及 9·8 得出

$$r'_{2k+2m+7}(N) = \int_0^1 \mathfrak{T}_0^{2k+3}(\alpha)\, \mathfrak{Q}^2(\alpha)\, e(-N\alpha)\, d\alpha =$$

$$= \sum_{q \leqslant L^\sigma} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} A^2 \left(\frac{W_{h,q}}{\varphi(q)}\right)^{2k+2m+7} e_q(-Nh)\, \Psi(N) + O(P^{k+3} L^{-\varepsilon_1} Q^2(0)),$$

此處

$$\Psi(N) = \sum_{\substack{n_1+\cdots+n_{2k+3}=N \\ P^k \leqslant n \leqslant (2P)^k}} \frac{1}{\prod_{i=1}^{2k+3} n_i^{1-\alpha} \log n_i}.$$

由引理 7·19, $\Psi(N)$ 適合於引理中的不等式. 由於

$$\sum_{q > L^\sigma} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \left(\frac{W_{h,q}}{\varphi(q)}\right)^{2k+2m+7} e_q(-Nh) \ll L^{-\varepsilon_1}$$

(如第七章的方法), 可以得出本引理.

定理 13 可由引理 9·9 及定理 12 得出之.

§4. Davenport 的引理

對較小的 k, 以上的結果可以更進一步使之精密. 以下著者將證明

$$H(4) \leqslant 15, \quad H(5) \leqslant 29, \quad H(6) \leqslant 37, \quad H(7) \leqslant 55, \quad H(8) \leqslant 75.$$

在證明這些結果時, 以下的 Davenport 的引理有重要作用.

引 理 9·10. (Davenport)*. 命 $\{M\}$ 表一自然數的集合(並不假定其互不相同),並假定它適合以下的條件:

a) 在 $\{M\}$ 中有 $\mathfrak{M}$ 對相等的元素，即 $M_1 = M_2$ $(M_1 \in \{M\}, M_2 \in \{M\})$ 的解答數等於 $\mathfrak{M}$;

б) $\{M\}$ 中的元素的個數是 $\mathfrak{N}$;

及

в) $\{M\}$ 中的元素適合於 $\leqslant P^\delta$.

命 $f(x)$ 代表一個 k 次整值多項式. 則方程

$$f(x_1) + M_1 = f(x_2) + M_2, \qquad P \leqslant x_1, x_2 \leqslant 2P, \qquad M_1, M_2 \in \{M\} \tag{1}$$

的解答的個數

$$\ll P^{1+\varepsilon}\mathfrak{M}\left(1 + P^{\delta-k+1-2^{-r+1}} + P^{(1-2^{-r})(\delta-k+1)-(r+1)2^{-r}}\mathfrak{M}^{-2^{-r}}\mathfrak{N}^{2^{1-r}}\right),$$

此處 r 適合於 $1 \leqslant r \leqslant k-2$, 而符號 $\ll$ 所涉及的常數僅依於 k 及 ε.

證: 引進符號

$$t_1 \Delta f(x) = f(x + t_1) - f(x)$$

及

$$t_1 \cdots t_r \Delta^r f(x) = t_r \Delta\left(t_1 \cdots t_{r-1} \Delta^{r-1} f(x)\right).$$

1) 命 $N_r (r \geqslant 1)$ 代表下式的解數:

$$\begin{gathered} t_1 \cdots t_r \Delta^r f(x) + M_1 = M, \\ P \leqslant x \leqslant 2P, \qquad t_1 \cdots t_r \ll P^{\delta-k+r}, \ t_i > 0. \end{gathered} \tag{2}$$

對已定的 $t_1, \cdots, t_r$ 及 M, (2) 式的解數用 $r(M, t)$ 表它. 今往證明

* Rao 對這引理提供了有價值的意見.

$$N_r \ll \mathfrak{M} P^{\delta-k+r+\varepsilon} + (\mathfrak{M} P^{\delta-k+r} N_{r+1})^{1/2}. \tag{3}$$

由 Cauchy 不等式可知

$$N_r = \sum_t \sum_M r(M, t) \leqslant \Big(\sum_t \sum_M 1\Big)^{1/2} \Big(\sum_t \sum_M r^2(M, t)\Big)^{1/2} \ll$$

$$\ll \Big(P^{\delta-k+r+\varepsilon} \mathfrak{M} \sum_t \sum_M r^2(M, t)\Big)^{1/2},$$

而 $\sum_t \sum_M r^2(M,t)$ 乃是下式的解數:

$$t_1 \cdots t_r \Delta^r f(x_1) + M_1 = t_1 \cdots t_r \Delta^r f(x_2) + M_2, \tag{4}$$

並且此式的雙方都限定在 $\{M\}$ 中. $t_1 \cdots t_r \Delta^r f(x_2) + M$ 在 $\{M\}$ 中的個數顯然就是 N_r. 因此, 當 $x_1 = x_2$ 時, (4) 式的解數是 N_r. 今假定 $x_1 > x_2$, 並命 $x_1 = x + t_{r+1}$ 及 $x_2 = x$, 則得

$$t_1 \cdots t_{r+1} \Delta^{r+1} f(x) + M_1 = M_2. \tag{5}$$

由於

$$\Delta^{r+1} f(x) \gg x^{k-r-1} \gg P^{k-r-1},$$

可知

$$t_1 \cdots t_{r+1} \ll P^{\delta-k+r+1}.$$

故適合 $x_1 > x_2$ 的 (4) 式的解數 $\ll N_{r+1}$. 因此得出

$$N_r \ll \{P^{\delta-k+r+\varepsilon} \mathfrak{M} (N_r + N_{r+1})\}^{1/2},$$

即

$$N_r \ll P^{\delta-k+r+\varepsilon} \mathfrak{M} + (P^{\delta-k+r+\varepsilon} \mathfrak{M} N_{r+1})^{1/2}.$$

2) 當 $1 \leqslant r \leqslant k-2$ 時,

$$N_1 \ll \mathfrak{M} P^{\delta-k+2-2^{-r+1}+\varepsilon} + \mathfrak{M}^{1-2^{-r}} P^{(\delta-k+1)(1-2^{-r})+1-(r+1)2^{-r}+\varepsilon} N_{r+1}^{2^{-r}}. \tag{6}$$

當 $r=1$ 時，(6) 式由 (3) 得出． 現在假定 (6) 式對 $r-1$ 是眞實的． 由 (3) 得出

$$N_1 \ll \mathfrak{M}\, P^{\delta-k+2-2^{-r+2}+\varepsilon} + \mathfrak{M}^{1-2^{-r+1}}\, P^{(\delta-k+1)(1-2^{-r+1})+1-r2^{-r+1}+\varepsilon}\, N_r^{2^{-r+1}} \ll$$

$$\ll \mathfrak{M}\, P^{\delta-k+2-2^{-r+2}+\varepsilon} + \mathfrak{M}^{1-2^{-r+1}}\, P^{(\delta-k+1)(1-2^{-r+1})+1-r2^{-r+1}+\varepsilon} \times$$

$$\times \left(\mathfrak{M}\, P^{\delta-k+r+\varepsilon} + (P^{\delta-k+r+\varepsilon}\, \mathfrak{M}\, N_{r+1})^{\frac{1}{2}}\right)^{2^{-r+1}} \ll$$

$$\ll \mathfrak{M}\, P^{\delta-k+2-2^{-r+1}+\varepsilon} + \mathfrak{M}^{1-2^{-r}}\, P^{(\delta-k+1)(1-2^{-r})+1-(r+1)2^{-r}+\varepsilon}\, N_{r+1}^{2^{-r}}.$$

3) 命 N 表 (1) 式的解數，今往證明

$$N \ll P\, \mathfrak{M} + N_1.$$

若 $x_1 = x_2$，則 (1) 的解數 $\ll P\,\mathfrak{M}$．當 $x_1 \neq x_2$，則 (1) 的解數 $\ll N_1$．

由 (6) 式及顯然的不等式

$$N_{r+1} \ll \sum_{M_1} \sum_{M_2} d^r(M_2 - M_1) \ll \mathfrak{M}^2 P^{\varepsilon}$$

而得出本引理．

附記： 在將來應用時，數集 $\{M\}$ 都是適合於條件 $\mathfrak{M} \ll \mathfrak{N}\, P^{\varepsilon}$ 者． 因之引理 9·10 的結論可以化簡成：

$$P^{1+\varepsilon}\, \mathfrak{N}\, (1 + P^{\delta-k+1-2^{-r+1}} + P^{(1-2^{-r})(\delta-k+1)-(r+1)2^{-r}}\, \mathfrak{M}^{2^{-r}}). \qquad (7)$$

引理 9·11. 命 $f(x)$ 代表一個四次的整值多項式． 則方程

$$f(x_1) + f(x_2) + f(x_3) + f(x_4) + f(x_4') = f(y_1) + f(y_2) + f(y_3) + f(y_4) + f(y_4'),$$

$$P \leqslant x_1, y_1 \leqslant 2P,\quad P^{\frac{132}{167}} \leqslant x_2, y_2 \leqslant 2P^{\frac{132}{167}},\quad P^{\frac{108}{167}} \leqslant x_3, y_3 \leqslant 2P^{\frac{108}{167}},$$
$$P^{\frac{90}{167}} \leqslant x_4, y_4, x_4', y_4' \leqslant 2P^{\frac{90}{167}},$$

的解數 $\ll P^{\frac{7}{2}+\frac{5}{334}+\varepsilon}$．

證：1）取 $\{M\}$ 是由以下形狀的整數所成的集合：

$$f(z_1)+f(z_1'),\quad P^{\frac{5}{6}}\leqslant z_1, z_1'\leqslant 2P^{\frac{5}{6}}.$$

則得 $\mathfrak{N}=P^{\frac{5}{3}}$，$\mathfrak{M}\ll P^{\frac{5}{3}+\varepsilon}$（由定理 4），$\delta=\frac{10}{3}$．今取 $r=1$，則由 (7) 式得出：方程

$$f(x_1)+f(x_2)+f(x_2')=f(y_1)+f(y_2)+f(y_2'),$$

$$P\leqslant x_1, y_1\leqslant 2P,\quad P^{\frac{5}{6}}\leqslant x_2, y_2, x_2', y_2'\leqslant 2P^{\frac{5}{6}},$$

的解數 $\ll P^{1+\frac{5}{3}+\varepsilon}=P^{\frac{8}{3}+\varepsilon}$．證明時用了：

$$\delta-k+1-2^{-r+1}=\frac{10}{3}-4+1-1=\frac{10}{3}-4<0$$

及

$$\left(1-\frac{1}{2^r}\right)(\delta-k+1)-(r+1)2^{-r}+2^{-r}\frac{5}{3}=\frac{1}{2}\left(\frac{10}{3}-4+1\right)-1+\frac{5}{6}=0.$$

2）取 $\{M\}$ 是由以下形狀的整數所成的集合：

$$f(z_1)+f(z_2)+f(z_2'),\quad P^{\frac{9}{11}}\leqslant z_1\leqslant 2P^{\frac{9}{11}},\quad P^{\frac{9}{11}\cdot\frac{5}{6}}\leqslant z_2, z_2'\leqslant 2P^{\frac{9}{11}\cdot\frac{5}{6}}.$$

由 1）可得 $\mathfrak{M}\ll P^{\frac{9}{11}+2\frac{9}{11}\frac{5}{6}+\varepsilon}=P^{\frac{24}{11}+\varepsilon}=\mathfrak{N}P^{\varepsilon}$ 及 $\delta=\frac{36}{11}$．今取 $r=2$，由 (7) 得出：方程

$$f(x_1)+f(x_2)+f(x_3)+f(x_3')=f(y_1)+f(y_2)+f(y_3)+f(y_3'),$$

$$P\leqslant x_1, y_1\leqslant 2P,\quad P^{\frac{9}{11}}\leqslant x_2, y_2\leqslant 2P^{\frac{9}{11}},$$

$$P^{\frac{9}{11}\cdot\frac{5}{6}}\leqslant x_3, y_3, x_3', y_3'\leqslant 2P^{\frac{9}{11}\cdot\frac{5}{6}},$$

的解數是 $\ll P^{1+\varepsilon}\mathfrak{M} \ll P^{1+\frac{24}{11}+\varepsilon} = P^{3+\frac{2}{11}+\varepsilon}$. (證明時用了:

$$\delta - k + 1 - 2^{-r+1} = \frac{36}{11} - 4 + 1 - \frac{1}{2} < 0,$$

$$\left(1-\frac{1}{2^r}\right)(\delta - k + 1) - (r+1)2^{-r} + 2^{-r}\cdot\frac{24}{11} =$$

$$= \frac{3}{4}\left(\frac{36}{11} - 3\right) - 3\cdot\frac{1}{4} + \frac{1}{4}\cdot\frac{24}{11} = 0.)$$

3) 再取 $\{M\}$ 是由以下形狀的整數所成的集合:

$$f(z_1) + f(z_2) + f(z_3) + f(z_3'),$$

$$P^{\frac{132}{167}} \leqslant z_1 \leqslant 2P^{\frac{132}{167}}, \quad P^{\frac{132}{167}\cdot\frac{9}{11}} \leqslant z_2 \leqslant 2P^{\frac{132}{167}\cdot\frac{9}{11}},$$

$$P^{\frac{132}{167}\cdot\frac{9}{11}\cdot\frac{5}{6}} \leqslant z_3, z_3' \leqslant 2P^{\frac{132}{167}\cdot\frac{9}{11}\cdot\frac{5}{6}}.$$

由 2) 已知

$$\mathfrak{M} \ll P^{\frac{132}{167}\left(3+\frac{2}{11}\right)+\varepsilon} = P^{\frac{420}{167}+\varepsilon} = \mathfrak{N} P^{\varepsilon}.$$

又 $\delta = \frac{4\cdot 132}{167}$. 今取 $r=2$, 並且由於

$$1 + \frac{420}{167} = \frac{587}{167} = \frac{7}{2} + \frac{5}{334},$$

$$\delta - k + 1 - 2^{-r+1} = \frac{4\cdot 132}{167} - 3 - \frac{1}{2} < 0$$

及

$$\left(1-\frac{1}{2^r}\right)(\delta - k + 1) - (r+1)2^{-r} + 2^{-r}\frac{420}{167} =$$

$$= \frac{3}{4}\left(\frac{4\cdot 132}{167} - 4 + 1\right) - \frac{3}{4} + \frac{1}{4}\cdot\frac{420}{167} = 0,$$

得出本引理.

爲了清楚起見,我們把這證明列爲下表:

$f(x)$ 的個數	r	λ	在 $\mathfrak{M}P$ 中 P 的方數
3	1	$\frac{5}{6}$	$1+2\cdot\frac{5}{6}+\varepsilon=\frac{8}{3}+\varepsilon$
4	2	$\frac{9}{11}$	$1+\frac{9}{11}\frac{8}{3}+\varepsilon=3+\frac{2}{11}+\varepsilon$
5	2	$\frac{132}{167}$	$1+\frac{132}{167}\left(3+\frac{2}{11}\right)+\varepsilon=\frac{7}{2}+\frac{5}{334}+\varepsilon$

引理 9·12. 命 $f(x)$ 表一五次的整值多項式. 方程

$$f(x_1)+\cdots+f(x_7)+f(x_7')=f(y_1)+\cdots+f(y_7)+f(y_7'),$$

$$P\leqslant x_1,y_1\leqslant 2P,$$

$$P^{\lambda_1}\leqslant x_2,y_2\leqslant 2P^{\lambda_1},\qquad \lambda_1=\frac{2\ 334\ 984}{2\ 873\ 111},$$

$$P^{\lambda_1\lambda_2}\leqslant x_3,y_3\leqslant 2P^{\lambda_1\lambda_2},\qquad \lambda_2=\frac{238\ 712}{291\ 873},$$

$$P^{\lambda_1\lambda_2\lambda_3}\leqslant x_4,y_4\leqslant 2P^{\lambda_1\lambda_2\lambda_3},\qquad \lambda_3=\frac{24\ 616}{29\ 839},$$

$$P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}}\leqslant x_5,y_5\leqslant 2P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}},$$

$$P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}}\leqslant x_6,y_6\leqslant 2P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}},$$

$$P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}\cdot\frac{15}{17}}\leqslant x_7,y_7,x_7',y_7'\leqslant 2P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}\cdot\frac{15}{17}}$$

的解數

$$\ll P^{\frac{9}{2}+\rho+\varepsilon},\qquad \rho=\frac{318\ 447}{5\ 746\ 222}.$$

這引理的證明可以用下表說明它:

$f(x)$ 的個數	r	λ	在 $\mathfrak{M}P$ 中 P 的方數
3	2	$\frac{15}{17}$	$\frac{47}{17}+\varepsilon$
8	3	—	$\frac{9}{2}+\rho+\varepsilon$

說明: $\frac{9}{2}+\rho$ 可由 $\sigma=\frac{47}{17}$ 經公式

$$\sigma'=1+\frac{32\sigma}{35+\sigma}$$

連續運用五次得出. 在計算時運用次式可以更爲便捷:

$$\frac{\sigma'+7}{\sigma'-5}=\frac{10}{7}\frac{\sigma+7}{\sigma-5}.$$

引理 9·13　命 $f(x)$ 代表六次整值多次式. 則有 $\mu_1,\cdots,\mu_{13}$ 存在,使方程

$$\sum_{\nu=1}^{13}f(x_\nu)=\sum_{\nu=1}^{13}f(y_\nu),\qquad P^{\mu_\nu}\leqslant x_\nu,y_\nu\leqslant 2P^{\mu_\nu},\ 1\leqslant\nu\leqslant 13,$$

的解數 $\ll P^{\mu_1+\cdots+\mu_{13}+\varepsilon}$, 而 $\mu_1+\cdots+\mu_{13}>5{,}689$.

此引理可由下表以證明之:

$f(x)$ 的個數	r	λ	在 $\mathfrak{M}P$ 中 P 的方數
3	2	$\frac{9}{10}$	$\frac{14}{5}+\varepsilon$
4	3	$\frac{195}{224}$	$\frac{55}{16}+\varepsilon$
5	3	$\frac{624}{727}$	$\frac{2872}{727}+\varepsilon$
13	4	—	5,689

說明：數值 5,689 可由 $\sigma = \frac{2872}{727}$ 經公式

$$\sigma' = 1 + \frac{80\,\sigma}{90+\sigma} \quad \left(\text{即}\ \frac{\sigma'+15}{\sigma'-6} = \frac{32}{25}\,\frac{\sigma+15}{\sigma-6}\right)$$

連續運用八次得出.

引理 9·14. 命 $f(x)$ 表一個七次整值多項式. 則有 $\mu_1, \cdots, \mu_{19}$ 存在使

$$\sum_{\nu=1}^{19} f(x_\nu) = \sum_{\nu=1}^{19} f(y_\nu), \qquad P^{\mu_\nu} \leqslant x_\nu, y_\nu \leqslant 2P^{\mu_\nu}, \qquad 1 \leqslant \nu \leqslant 19,$$

的解數 $\ll P^{\mu_1+\cdots+\mu_{19}+\epsilon}$, 此處 $\mu_1 + \cdots + \mu_{19} > 6{,}767$.

此引理可由下表以證明之：

$f(x)$ 的個數	r	λ	在 $\mathfrak{M}P$ 中 P 的方數
3	2	$\frac{21}{23}$	$\frac{65}{23} + \epsilon$
4	3	$\frac{529}{596}$	$\frac{2091}{596} + \epsilon$
5	3	$\frac{27\,416}{31\,295}$	$\frac{127\,481}{31\,295} + \epsilon$
6	4	$\frac{3\,973\,025}{3\,413\,456}$	$\frac{15\,524\,151}{3\,413\,456} + \epsilon$
7	4	$\frac{324\,278\,320}{373\,937\,071}$	$\frac{1\,848\,731\,376}{373\,937\,031} + \epsilon$
19	5	—	6,767

說明：數值 6,767 是由 $\sigma = \frac{1\,848\,731\,376}{373\,937\,031}$ 經公式

$$\sigma' = 1 + \frac{192\,\sigma}{217+\sigma} \quad \left(\text{即}\ \frac{\sigma'+31}{\sigma'-7} = \frac{112}{93}\,\frac{\sigma+31}{\sigma-7}\right)$$

連續運用十二次得來的.

引 理 9·15　命 $f(x)$ 表一個八次整值多項式，則有 $\mu_1, \cdots, \mu_{29}$ 存在，使

$$\sum_{\nu=1}^{29} f(x_\nu) = \sum_{\nu=1}^{29} f(y_\nu), \qquad P^{\mu_\nu} \leqslant x_\nu, y_\nu \leqslant 2P^{\mu_\nu}, \qquad 1 \leqslant \nu \leqslant 29,$$

的解數 $\ll P^{\mu_1+\cdots+\mu_{29}+\varepsilon}$，此處 $\mu_1 + \cdots + \mu_{29} > 7,8887$.

此引理可由下表以證明之：

$f(x)$ 的個數	r	λ	在 $\mathfrak{M}P$ 中 P 的方數
3	2	$\frac{12}{13}$	$\frac{37}{13}+\varepsilon$
4	3	$\frac{689}{765}$	$\frac{2\,726}{765}+\varepsilon$
5	4	$\frac{42\,075}{47\,263}$	$\frac{197\,193}{47\,263}+\varepsilon$
6	4	$\frac{5\,198\,930}{5\,868\,753}$	$\frac{27\,559\,983}{5\,868\,753}+\varepsilon$
7	5	$\frac{1\,308\,731\,914}{1\,483\,010\,727}$	$\frac{7\,618\,886\,936}{1\,483\,010\,727}+\varepsilon$
8	5	$\frac{330\,711\,392\,121}{375\,405\,547\,232}$	$\frac{259\,302\,166\,745}{46\,925\,693\,404}+\varepsilon$
9	5	$\frac{10\,464\,489\,629\,092}{11\,896\,378\,130\,937}$	$\frac{69\,720\,761\,315\,192}{11\,896\,378\,130\,437}+\varepsilon$
29	6	—	7,8887

說明：數值 7,8887 是由 $\sigma = \frac{69\,720\,761\,315\,192}{11\,896\,378\,130\,437}$ 經公式

$$\sigma' = 1 - \frac{448\,\sigma}{504+\sigma} \left(即\ \frac{\sigma'+63}{\sigma'-8} = \frac{512}{441}\,\frac{\sigma+63}{\sigma-8} \right)$$

連續應用二十次得來的.

附記：當 $k > 8$ 還有其他的方法得出更精密的結果. 因此我們的計算終止於 $k = 8$.

§5. 不等式 $H(4)\leqslant 15$ 的證明

命

$$T_0(\alpha)=T(\alpha,P)=\sum_{P<n\leqslant 2P}e(n^4\alpha),$$

$$T'(\alpha)=T(\alpha,P^{\frac{132}{167}}),$$

$$T''(\alpha)=T(\alpha,P^{\frac{108}{167}}),$$

$$T'''(\alpha)=T(\alpha,P^{\frac{90}{167}}),$$

$$Q(\alpha)=T'(\alpha)T''(\alpha)T'''^2(\alpha),$$

$$R(\alpha)=T_0(\alpha)Q(\alpha).$$

由於

$$\frac{132}{167}+\frac{108}{167}+2\cdot\frac{90}{168}=\frac{5}{2}+\frac{5}{334},$$

得出

$$P^{\frac{5}{2}+\frac{5}{334}}\ll Q(0)\ll P^{\frac{5}{2}+\frac{5}{334}}.$$

如第七章 §3 的方法來分割隔間 $-\frac{1}{\tau}\leqslant\alpha\leqslant 1-\frac{1}{\tau}$.

引理 9·16.

$$\int_E|T_0^2(\alpha)R(\alpha)|^2d\alpha\ll Q^2(0)P^{2-\frac{5}{334}+\varepsilon}.$$

證: 由引理 9·11 及 3·6 得出

$$\int_E|T_0^2(\alpha)R(\alpha)|^2d\alpha\ll P^{\frac{7}{8}\cdot 4+\varepsilon}\int_0^1|R(\alpha)|^2d\alpha\ll$$

$$\ll P^{\frac{7}{2}+\frac{7}{2}+\frac{5}{334}+\varepsilon}\ll Q^2(0)P^{2-\frac{5}{334}+\varepsilon}.$$

引 理 9·17.

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} | T_0^2 (\alpha) R (\alpha) |^2 d\alpha \ll Q^2 (0) P^2 .$$

證: 把隔間 $\mathfrak{M} = \mathfrak{M}(h,q)$ 分為兩類:

$$\mathfrak{M}_1: \qquad q \leqslant P^{\frac{9}{14}},$$

$$\mathfrak{M}_2: \qquad P^{\frac{9}{14}} < q \leqslant P^{1+\varepsilon}.$$

在 $\mathfrak{M}_2$ 上應用引理 7·10 及 7·11 可得

$$\begin{aligned} T_0 (\alpha) &\ll q^{\frac{3}{4}+\varepsilon} + q^{-\frac{1}{4}+\varepsilon} P \ll \\ &\ll P^{\frac{3}{4}+\varepsilon} + P^{1-\frac{1}{4}\cdot\frac{9}{14}+\varepsilon} \ll \\ &\ll P^{\frac{7}{8}+\varepsilon} . \end{aligned}$$

如引理 9·3 得出

$$\begin{aligned} \sum_{\mathfrak{M}_2} \int_{\mathfrak{M}_2} | T_0^2 (\alpha) R (\alpha) |^2 d\alpha &\ll P^{\frac{7}{2}+\epsilon} \int_0^1 | R (\alpha) |^2 d\alpha \ll \\ &\ll Q^2 (0) P^{2-\frac{5}{334}+\epsilon} . \end{aligned}$$

又把引理 7·10 及 7·11 用到 $\mathfrak{M}_1$ 上,則當 α 在 $\mathfrak{M}_1$ 上,得

$$\begin{aligned} T_0 (\alpha) &\ll q^{1-\frac{1}{4}+\varepsilon} + q^{-\frac{1}{4}+\varepsilon} \min (P, |\beta|^{-\frac{1}{4}}) \ll \\ &\ll q^{-\frac{1}{4}+\varepsilon} \min (P, |\beta|^{-\frac{1}{4}}), \end{aligned}$$

$$T' (\alpha) \ll q^{-\frac{1}{4}+\epsilon} P^{\frac{132}{167}},$$

$$T'' (\alpha) \ll q^{-\frac{1}{4}+\epsilon} P^{\frac{108}{167}}.$$

於是

$$\sum_{\mathfrak{M}_1}\int_{\mathfrak{M}_1}|T_0^6(\alpha)\,T'^2(\alpha)\,T''^2(\alpha)|\,d\alpha \ll \sum_q q\cdot q^{-\frac{10}{4}}P^{\frac{132}{167}\cdot 2}P^{\frac{108}{167}\cdot 2}\int_{\mathfrak{M}}\min(1,|\beta|^{-\frac{1}{4}})^9\,d\beta \ll$$

$$\ll \sum_q q^{-\frac{3}{2}+\epsilon}P^{2\cdot\frac{132}{167}+2\cdot\frac{108}{167}+6-4} \ll$$

$$\ll P^{2\cdot\frac{132}{167}+2\cdot\frac{108}{167}+2}.$$

因此得出

$$\sum_{\mathfrak{M}_1}\int_{\mathfrak{M}_1}|T_0^6(\alpha)\,T'^2(\alpha)\,T''^2(\alpha)\,T'''^4(\alpha)|\,d\alpha \ll T'''^4(0)\sum_{\mathfrak{M}_1}\int_{\mathfrak{M}_1}|T_0^6(\alpha)\,T'^2(\alpha)\,T''^2(\alpha)|\,d\alpha$$

$$\ll Q^2(0)\,P^2.$$

引理 9·18.

$$\int_0^1 |T_0^2(\alpha)\,R(\alpha)|^2\,d\alpha \ll Q^2(0)\,P^2.$$

這引理由引理 9·16 及 9·17 直接得出.

如 §3 的方法,我們易於得出以下的結論: 以 $r'_{15}(N)$ 表下列方程的解數:

$$p_1^4+p_2^4+\cdots+p_{15}^4=N,$$

此處 $p_1,\cdots,p_{15}$ 是素數,適合於

$$P\leqslant p_\nu\leqslant 2P,\ 1\leqslant\nu\leqslant 7,\qquad P^{\frac{132}{167}}\leqslant p_8,p_9\leqslant 2P^{\frac{132}{167}},$$

$$P^{\frac{108}{167}}\leqslant p_{10},p_{11}\leqslant 2P^{\frac{108}{167}},\qquad P^{\frac{90}{167}}\leqslant p_{12},p_{13},p_{14},p_{15}\leqslant 2P^{\frac{90}{167}},$$

則

$$r'_{15}(N)=\mathfrak{S}(N)\,\Psi_1(N)+O(P^3Q^2(0)L^{-16}),$$

此處

$$\frac{P^3 Q^2(0)}{L^{15}} \ll \Psi_1(N) \ll \frac{P^3 Q^2(0)}{L^{15}}.$$

由此得出

定 理 14. 所有的充分大的 $\equiv 15 \pmod{240}$ 的整數 N, 是 15 個素數的四次方之和,卽

$$H(4) \leqslant 15.$$

§6. 不等式 $H(5) \leqslant 25$ 的證明

一如 §5 的方法,我們可以不難得出以下的結果:

命 $r'_{25}(N)$ 表示下列方程的解數:

$$p_1^5 + p_2^5 + \cdots + p_{25}^5 = N,$$

此處 $p_1, \cdots, p_{25}$ 是素數,且適合於

$$P \leqslant p_\nu \leqslant 2P, \qquad 1 \leqslant \nu \leqslant 11,$$

$$P^{\lambda_1} \leqslant p_{12}, p_{13} \leqslant 2P^{\lambda_1}, \qquad \lambda_1 = \frac{2\ 334\ 984}{2\ 873\ 111},$$

$$P^{\lambda_1\lambda_2} \leqslant p_{14}, p_{15} \leqslant 2P^{\lambda_1\lambda_2}, \qquad \lambda_2 = \frac{238\ 712}{291\ 873},$$

$$P^{\lambda_1\lambda_2\lambda_3} \leqslant p_{16}, p_{17} \leqslant 2P^{\lambda_1\lambda_2\lambda_3}, \qquad \lambda_3 = \frac{24\ 616}{29\ 839},$$

$$P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}} \leqslant p_{18}, p_{19} \leqslant 2P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}},$$

$$P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}} \leqslant p_{20}, p_{21} \leqslant 2P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}},$$

$$P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}\cdot\frac{15}{17}} \leqslant p_{22}, p_{23}, p_{24}, p_{25} \leqslant 2P^{\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}\cdot\frac{15}{17}}.$$

則

$$r'_{25}(N) = \mathfrak{S}(N)\Psi_2(N)\left(1 + O\left(\frac{1}{L}\right)\right),$$

此處

$$\Psi_2(N) \underset{\gg}{\ll} P^{6+\lambda_1+\lambda_1\lambda_2+\lambda_1\lambda_2\lambda_3+\lambda_1\lambda_2\lambda_3\frac{2568}{3077}+\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}+2\lambda_1\lambda_2\lambda_3\frac{2568}{3077}\cdot\frac{272}{321}\cdot\frac{15}{17}} L^{-25}.$$

由此得出

定 理 15. 所有的充分大的奇數可以表成二十五個素數的五次方的和．即 $H(5) \leqslant 25$.

今不再重複以下各式的證明：$H(6) \leqslant 37$，$H(7) \leqslant 55$ 及 $H(8) \leqslant 75$.

第 十 章

素數未知數的不定方程組*

§1.

在本章及下一章中將討論不定方程組:

$$p_1^k + \cdots + p_s^k = N_k,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$p_1 + \cdots + p_s = N_1,$$

其中未知數 $p_1, \cdots, p_s$ 是素數. 本章中將給與此方程組的解數的漸近式,而假定了 $s \geqslant s_0$, 此 s_0 的數值如下表:

k	2	3	4	5	6	7	8	$\geqslant 9$
s_0	7	19	49	127	315	763	1781	$2k^2(3\log k + \log\log k + 4)$

爲了免除瑣碎的枝節運算,我們的證明中將假定 $k \geqslant 3$. 關於 $k=2$ 的情況,讀者可以依據這一證明,做適當的而不困難的修整,得出證明.

§2. 證明定理 16 所需要的幾條引理

引 理 10·1.** 命 $\gamma_k, \cdots, \gamma_1$ 表 k 個實數. 且命

---

* 關於第十章及第十一章中所討論的問題可比較 К. К. Марджанишвили „Об одной задаче аддитивной теории чисел“. Изв. АН СССР, Серия математическая, Т. 4 (1940), стр. 193-194. (俄文本譯者註).

** И. М. Виноградов, *Математический Сборник*, 3 (1938), 435－471; 這一證明見華羅庚,等冪和問題解數的研究,數學學報, 2 (1952).

$$I = \int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\,dx,$$

則

$$I \ll Z, \qquad Z = (\max(1, |\gamma_1|, \cdots, |\gamma_k|))^{-\sigma}.$$

證：顯然 $|I| \leqslant 1$. 故可假定 $|\gamma_k| \geqslant 1$. 我們有

$$I^k = \int_0^1 \cdots \int_0^1 e(\psi)\,dx_1 \cdots dx_k,$$

此處

$$\psi = (x_1^k + \cdots + x_k^k)\gamma_k + \cdots + (x_1 + \cdots + x_k)\gamma_1.$$

顯然有

$$I^k = k! \int\cdots\int_{0 \leqslant x_k \leqslant x_{k-1} \leqslant \cdots \leqslant x_1 \leqslant 1} e(\psi)\,dx_1 \cdots dx_k.$$

今討論變換

$$\left.\begin{array}{c} (x_1^k + \cdots + x_k^k)\,|\gamma_k| = y_k \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ (x_1 + \cdots + x_k)\,|\gamma_1| = y_1 \end{array}\right\}.$$

以 $\mathfrak{N}$ 代表當 $x_1, \cdots, x_k$ 屬於域 $0 \leqslant x_k \leqslant x_{k-1} \leqslant \cdots \leqslant x_1 \leqslant 1$ 時 $y_1, \cdots, y_k$ 所繪出的域. 此變換的函數行列式

$$\frac{\partial(x_1, \cdots, x_k)}{\partial(y_1, \cdots, y_k)} = g(y_1, \cdots, y_k)$$

經常是正號. 引用引理 7·5 可得

$$|k!^{-1} I^k| = \left| \int\cdots\int_{\mathfrak{N}} e(\pm y_k \pm \cdots \pm y_1)\, g(y_1, \cdots, y_k)\,dy_1 \cdots dy_k \right| \leqslant$$

$$\leqslant \int\cdots\int dy_1 \cdots dy_{h-1}\,dy_{h+1} \cdots dy_k \left| \int e(\pm y_h)\, g(y_1, \cdots, y_k)\,dy_h \right| \ll$$

$$\ll \max_{0 \leqslant \xi \leqslant 1} \int\cdots\int dy_1 \cdots dy_{h-1}\,dy_{h+1} \cdots dy_k \int_{v \leqslant y_h \leqslant v+\xi} g(y_1, \cdots, y_k)\,dy_h \ll$$

$$\ll \max_{0\leqslant\xi\leqslant 1} \underset{v\leqslant y_h\leqslant v+\xi}{\int_0^1\cdots\int_0^1} dx_1\cdots dx_k. \tag{1}$$

今有

$$\underset{v\leqslant y_h\leqslant v+\xi}{\int_0^1\cdots\int_0^1} dx_1\cdots dx_k \leqslant \underset{v\leqslant y_h\leqslant v+\xi}{\int\cdots\int} dx_1\cdots dx_k \leqslant \underset{v\leqslant y_h\leqslant v+1}{\int\cdots\int} dx_1\cdots dx_k =$$

$$= V(v+1)-V(v), \tag{2}$$

此處 $V(v)$ 是由

$$y_h = |\gamma_h|(x_1^h+\cdots+x_k^h)\leqslant v, \quad x_\nu\geqslant 0,$$

所定義的域的體積. 因

$$V(v)=\eta\left(\frac{v}{|\gamma_h|}\right)^{k/h}$$

(此處 η 是一僅依於 h 及 k 的常數),所以

$$V(v+1)-V(v)\ll\left(\frac{v+1}{|\gamma_h|}\right)^{k/h}-\left(\frac{v}{|\gamma_h|}\right)^{k/h}\ll$$

$$\ll|\gamma_h|^{-k/h}\int_v^{v+1}t^{k/h-1}\,dt\ll$$

$$\ll|\gamma_h|^{-k/h}(v+1)^{k/h-1}\ll$$

$$\ll|\gamma_h|^{-k/h}(|\gamma_h|k+1)^{k/h-1}. \tag{3}$$

(其中用 $v\leqslant k|\gamma_h|$). 綜合 (1), (2) 及 (3), 可得

$$I^k\ll|\gamma_h|^{-k/h}(|\gamma_h|k+1)^{k/h-1}\ll$$

$$\ll|\gamma_h|^{-k/h-1+k/h}=|\gamma_h|^{-1}.$$

這證明了本引理.

引理 10·2. 仍如引理 10·1 的假定，命 $\delta_\nu=\max(1,\gamma_\nu)$，則

$$I \ll \prod_{\nu=1}^{k} \delta_\nu^{-a^2}.$$

又當 $0<\delta\leqslant 1$ 時，

$$\int_0^\delta e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx \ll \prod_{\nu=1}^{k} \delta_\nu^{-a^2}.$$

又當 $g>k^2$ 時，

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} |I|^g\, d\gamma_k\cdots d\gamma_1$$

收斂.

證：由於

$$\prod_{\nu=1}^{k}\delta_\nu=\prod_{\nu=1}^{k}\max(1,|\gamma_\nu|)\leqslant \max(1,|\gamma_1|,\cdots,|\gamma_k|)^k,$$

故由引理 10·1 立刻得出第一個不等式.

再，

$$\int_0^\delta e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx=\delta\int_0^1 e(\gamma_k\delta^k y^k+\cdots+\gamma_1\delta y)\,dy \ll$$

$$\ll \delta\left(\prod_{\nu=1}^{k}\max(1,\delta^\nu|\gamma_\nu|)\right)^{-a^2} \ll$$

$$\ll \delta\left(\prod_{\nu=1}^{k}\max(\delta^\nu,\delta^\nu|\gamma_\nu|)\right)^{-a^2} \ll$$

$$\ll \delta^{\frac{1}{2}-\frac{1}{2}a}\left(\prod_{\nu=1}^{k}\delta_\nu\right)^{-a^2} \ll \left(\prod_{\nu=1}^{k}\delta_\nu\right)^{-a^2}.$$

這就證明了第二個不等式.

又積分

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|I|^g\,d\gamma_k\cdots d\gamma_1 \ll \prod_{\nu=1}^{k}\int_{-\infty}^{\infty}\delta_\nu^{-a^2 g}\,d\gamma_\nu$$

當 $g>k^2$ 時顯然收斂.

引 理 10·3. 命 $q_1,\cdots,q_k$ 是正整數，$H=q_1\cdots q_k$，又命 Q 代表 $q_1,\cdots,q_k$ 的最小公倍數，

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{H}\sum_{y=1}^{H}e\left(\frac{h_k}{q_k}y^k+\cdots+\frac{h_1}{q_1}y\right),\ (h_\nu,q_\nu)=1,$$

則

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\ll Q^{-a+\varepsilon},$$

且級數

$$\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^g$$

當 $g>k(k+1)$ 時收斂.

證：先證明

$$\left(\frac{h_k}{q_k}Q,\cdots,\frac{h_1}{q_1}Q,Q\right)=1.$$

若不然，必有一素數 p 使

$$p\left|\left(\frac{h_k}{q_k}Q,\cdots,\frac{h_1}{q_1}Q,Q\right)\right..$$

假定 p^b 能整除 Q，而 p^{b+1} 不能整除 Q. 由 Q 的定義，必有一 q，命之爲 q_l，能爲 p^b 所整除，但不能爲 p^{b+1} 所整除，卽 $\frac{h_l}{q_l}Q$ 不是 p 的倍數. 這和以上的假定相違.

由定理 1 可知

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{Q}\sum_{x=1}^{Q}e\left(g(x)/Q\right)\ll Q^{-a+\varepsilon}.$$

由此推得,引理中所討論的無窮級數

$$\ll \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{h_1} \cdots \sum_{h_k} Q^{-ag+\varepsilon} \leqslant \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} q_1 \cdots q_k Q^{-ag+\varepsilon}.$$

對一固定的 Q,我們來討論和

$$\sigma(Q) = \sum \cdots \sum q_1 \cdots q_k,$$

此和經過所有可能的最小公倍數爲 Q 的整數組 $q_1, \cdots, q_k$. 由引理 2·1 可知

$$\sigma(Q) \leqslant \Big(\sum_{q|Q} q\Big)^k \ll Q^k (d(Q))^k \ll Q^{k+\varepsilon}.$$

所以該級數

$$\ll \sum_{Q=1}^{\infty} Q^{k-ag+\varepsilon}.$$

顯然當 $k-ag<-1$ 時,此級數收斂,即 $g > k(k+1)$ 時,原級數收斂.

附 記: 引理 10·2 及 10·3 的收斂指數都還可改善. 請參考數學學報第二卷華羅庚著文.

引 理 10·4. 命

$$f(x) = \frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x, \quad (h_\nu, q_\nu) = 1, \quad q_\nu \geqslant 1.$$

又命 Q_1 是 $q_k, \cdots, q_2$ 的最小公倍數, Q 是 Q_1 及 q_1 的最小公倍數. 假定 $Q_1 < Q$, 則

$$\sum_{x=1}^{P} e(f(x)) \ll Q.$$

證：當 $Q \geqslant P$ 時，這引理顯然正確．假定 $Q < P$．命 $x = Q_1 y + z$，此處

$$1 \leqslant z \leqslant Q_1, \quad 0 \leqslant y \leqslant (P-z)/Q_1.$$

因為 q_1 不能整除 Q_1，所以

$$\left|\sum_{x=1}^{P} e(f(x))\right| = \left|\sum_{z=1}^{Q_1} e(f(z)) \sum_{y=1}^{(P-z)/Q_1} e^{2\pi i h_1 Q_1 y/q_1}\right| \leqslant$$

$$\leqslant Q_1 \max_z \left|\sum_y e^{2\pi i h_1 Q_1 y/q_1}\right| \leqslant$$

$$\leqslant \frac{Q_1}{\{h_1 Q_1/q_1\}} \leqslant \frac{Q_1 q_1}{(Q_1, q_1)} = Q.$$

（用了引理 1·8）．

引理 10·5. 命 σ 是一小於 $\frac{1}{4}a$ 的正數，及

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x.$$

又命

$$\alpha_\nu = \frac{h_\nu}{q_\nu} + \frac{\theta_\nu}{q_\nu \tau_\nu}, \quad |\theta_\nu| \leqslant 1, \quad (h_\nu, q_\nu) = 1,$$

其中

$$\tau_1 = P^{\frac{1}{2}}, \quad \tau_\nu = P^{\nu - \frac{1}{2}a + \sigma}, \quad 2 \leqslant \nu \leqslant k.$$

假定

$$P^{\frac{1}{2} - \frac{1}{2}a + \sigma} < q_1 \leqslant \tau_1, \quad q_\nu \leqslant P^{\frac{1}{2}a - 2\sigma}, \quad 2 \leqslant \nu \leqslant k,$$

則

$$\sum_{x=1}^{P} e(f(x)) \ll P^{1-\sigma}.$$

證：命

$$S_n = \sum_{x \leqslant n} e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x\right).$$

由於 $Q_1 \leqslant q_2 \cdots q_k < P^{(k-1)(\frac{1}{2}a-2\sigma)} = P^{\frac{1}{2}-\frac{1}{2}a-2\sigma(k-1)} < P^{\frac{1}{2}-\frac{1}{2}a+\sigma} < q_1$, 根據引理 10·4, 可知

$$S_n \ll Q \leqslant q_1 \cdots q_k \leqslant$$

$$\leqslant P^{\frac{1}{2}} \cdot P^{(\frac{1}{2}a-2\sigma)(k-1)} \ll P^{1-\frac{1}{2}a-2\sigma(k-1)}.$$

又

$$\sum_{x=1}^{P} e(f(x)) = \sum_{n=1}^{P} (S_n - S_{n-1}) e(\beta_k x^k + \cdots + \beta_1 x) =$$

$$= \sum_{n=1}^{P} S_n (e(\beta_k n^k + \cdots + \beta_1 n) - e(\beta_k (n+1)^k + \cdots + \beta_1 (n+1))) +$$

$$+ S_P e(\beta_k (P+1)^k + \cdots + \beta_1 (P+1)).$$

因爲

$$|e(\beta_k (n+1)^k + \cdots + \beta_1 (n+1)) - e(\beta_k n^k + \cdots + \beta_1 n)| \ll$$

$$\ll |\beta_k| P^{k-1} + |\beta_{k-1}| P^{k-2} + \cdots + |\beta_1| \ll$$

$$\ll \frac{P^{k-1}}{\tau_k} + \frac{P^{k-2}}{\tau_{k-1}} + \cdots + \frac{P}{\tau_2} + \frac{1}{q_1 \tau_1} \ll$$

$$\ll P^{-1+\frac{1}{2}a-\sigma} + P^{-\frac{1}{2}-\frac{1}{k}+\frac{1}{2}a-\sigma} \ll P^{-1+\frac{1}{2}a-\sigma},$$

所以

$$\sum_{x=1}^{P} e(f(x)) \ll \sum P^{1-\frac{1}{2}a-2\sigma(k-1)} P^{-1+\frac{1}{2}a-\sigma} \ll$$

$$\ll P^{1-\sigma(2k-1)} \ll P^{1-\sigma}.$$

§3. 關於 Tarry 問題的結果

定理 16. 命

$$S(\alpha_k, \cdots, \alpha_1) = \sum_{x \leqslant P} e(\alpha_k x^k + \cdots + \alpha_1 x).$$

命 t_0 表一與 k 有關的正整數，它的定義如下表：

k	2	3	4	5	6	7	8	$\geqslant 9$
t_0	3	8	23	62	156	380	889	$[k^2(3\log k+\log\log k+4)]-2$

則當 $t>t_0$ 時，有下面的結果

$$T(P)=\int_0^1\cdots\int_0^1|S(\alpha_k,\cdots,\alpha_1)|^{2t}\,d\alpha_k\cdots d\alpha_1=$$

$$=c_1c_2P^{2t-\frac{1}{2}k(k+1)}+O\left(P^{2t-\frac{1}{2}k(k+1)-c(k)}\right),$$

此處

$$c_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left|\int_0^1 e(\beta_kx^k+\cdots+\beta_1x)\,dx\right|^{2t}d\beta_k\cdots d\beta_1$$

及

$$c_2=\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{\infty}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{\infty}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t},$$

而

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{q_1\cdots q_k}\sum_{x=1}^{q_1\cdots q_k}B\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right).$$

證：1）由於 $S(\alpha_k,\cdots,\alpha_1)$ 的週期性，我們有

$$T(P)=\int_{-\frac{1}{\tau_1}}^{1-\frac{1}{\tau_1}}d\alpha_1\cdots\int_{-\frac{1}{\tau_k}}^{1-\frac{1}{\tau_k}}|S(\alpha_k,\cdots,\alpha_1)|^{2t}\,d\alpha_k.$$

今取

$$\tau_1=P^{\frac{1}{2}},\quad \tau_\nu=P^{\nu-\frac{1}{2}a+\sigma},\quad 2\leqslant\nu\leqslant k,$$

而 $\sigma=a^3$.

由引理7·1可知,對k維空間之每一點$(\alpha_k,\cdots,\alpha_1)$,我們有一有理點$\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$使

$$\alpha_\nu = \frac{h_\nu}{q_\nu} + \beta_\nu, \quad (h_\nu, q_\nu) = 1, \quad |\beta_\nu| \leqslant \frac{1}{q_\nu \tau_\nu}, \quad 0 < q_\nu \leqslant \tau_\nu.$$

我們現在注意所有適合條件

$$1 \leqslant q_\nu \leqslant P^{\frac{1}{2}a-2\sigma}\ (2 \leqslant \nu \leqslant k), \quad 1 \leqslant q_1 \leqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma}$$

的有理點. 對應於這樣的一點$\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$,我們做一$k$維空間的間隔: 這間隔是由適合

$$|\beta_\nu| \leqslant \frac{1}{q_\nu \tau_\nu}, \quad 1 \leqslant \nu \leqslant k.$$

的諸$(\alpha_k,\cdots,\alpha_1)$所成的. 這一間隔用$\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$來表它.

易於證明並無兩個$\mathfrak{M}$有公共點. 如若不然,假定

$$\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right) \text{ 及 } \mathfrak{M}\left(\frac{h'_k}{q'_k},\cdots,\frac{h'_1}{q'_1}\right)$$

有公共點. 因為間隔不同,所以必有一ν使$\frac{h_\nu}{q_\nu} \neq \frac{h'_\nu}{q'_\nu}$,且

$$\frac{1}{q_\nu q'_\nu} \leqslant \frac{|h_\nu q'_\nu - h'_\nu q_\nu|}{q_\nu q'_\nu} = \left|\frac{h_\nu}{q_\nu} - \frac{h'_\nu}{q'_\nu}\right| \leqslant \frac{1}{q_\nu \tau_\nu} + \frac{1}{q'_\nu \tau'_\nu} \leqslant$$

$$\leqslant \frac{2}{\tau_\nu} \max\left(\frac{1}{q_\nu}, \frac{1}{q'_\nu}\right),$$

也就是

$$\tau_\nu \leqslant 2\max(q_\nu, q'_\nu) \leqslant \begin{cases} 2P^{\frac{1}{2}a-2\sigma} & \text{當 } \nu > 1, \\ 2P^{\frac{1}{2}-\frac{1}{2}a+\sigma} & \text{當 } \nu = 1. \end{cases}$$

這是不可能的.

用 E 表示由

$$-\frac{1}{\tau_\nu}\leqslant\alpha_\nu\leqslant 1-\frac{1}{\tau_\nu},\quad 1\leqslant\nu\leqslant k,$$

中除去諸 $\mathfrak{M}$ 之後所餘下的部份．命

$$T_{(1)}=\int\cdots\int_E|S(\alpha_k,\cdots,\alpha_1)|^{2t}d\alpha_1\cdots d\alpha_k$$

及

$$T_{(2)}=\sum_{\mathfrak{M}}K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right),$$

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\int\cdots\int_{\mathfrak{M}}|S|^{2t}d\alpha_1\cdots d\alpha_k,$$

則

$$T(P)=T_{(1)}+T_{(2)}. \tag{1}$$

2）命 $H=q_1\cdots q_k$ 及

$$x=H\xi+\eta,\qquad \eta=1,\cdots,H,\qquad -\eta/H<\xi\leqslant(P-\eta)/H,$$

則在 $\mathfrak{M}\left(\frac{h_1}{q_1},\cdots,\frac{h_k}{q_k}\right)$ 上

$$S(\alpha_k,\cdots,\alpha_1)=\sum_\eta W_\eta e\left(\frac{h_k}{q_k}\eta^k+\cdots+\frac{h_1}{q_1}\eta\right),$$

此處

$$W_\eta=\sum_{-\frac{\eta}{H}\leqslant\xi\leqslant\frac{P-\eta}{H}}e(\beta_k(H\xi+\eta)^k+\cdots+\beta_1(H\xi+\eta)).$$

命

$$\varphi(\xi)=\beta_k(H\xi+\eta)^k+\cdots+\beta_1(H\xi+\eta),$$

則當 P 充分大時，

$$|\varphi'(\xi)| \leqslant \frac{kHP^{k-1}}{q_k\tau_k} + \cdots + \frac{H}{q_1\tau_1} \ll$$

$$\ll \sum_{\nu=2}^{k} P^{(\frac{1}{2}a-2\sigma)(k-2)} P^{\frac{1}{2}-\frac{1}{2}a+\sigma} \frac{P^{\nu-1}}{P^{\nu-\frac{1}{2}a+\sigma}} + P^{(\frac{1}{2}a-2\sigma)(k-1)} \frac{1}{P^{\frac{1}{2}}} \ll$$

$$\ll P^{-a-2\sigma(k-2)} + P^{-\frac{1}{2}a-2\sigma(k-1)} = o(1),$$

卽當 P 充分大時，$|\varphi'(\xi)| \leqslant \frac{1}{2}$. 故由引理 7·5 2) 可知

$$W_\eta = \int_{-\eta/H}^{(P-\eta)/H} e(\varphi(z))\,dz + O(1).$$

命 $x = P^{-1}(ZH+\eta)$，$\gamma_\nu = \beta_\nu P^\nu$ $(1 \leqslant \nu \leqslant k)$，可得

$$W_\eta = \frac{P}{H} R + O(1),$$

此處

$$R = \int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\,dx.$$

因此

$$S = B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) P R + O(H). \tag{2}$$

3) 因

$$Q \geqslant \max(q_1, \cdots, q_k) \geqslant (q_1 \cdots q_k)^a = H^a,$$

故由引理 10·1 及 10·2 可知

$$B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) P R \ll P Q^{-a+\varepsilon} Z \ll P H^{-a^2+\varepsilon} Z. \tag{3}$$

又當 α 在 $\mathfrak{M}$ 上，

$$H = q_1 \cdots q_k \leqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma+(k-1)(\frac{1}{2}a-2\sigma)} \leqslant$$

$$\leqslant P^{1-a-(2k-1)\sigma} \leqslant P^{1-a}$$

及

$$Z = \min(1, |\gamma_1|^{-a}, \cdots, |\gamma_k|^{-a}) =$$

$$= \min(1, (P|\beta_1|)^{-a}, \cdots, (P^k|\beta_k|)^{-a}) \geqslant$$

$$\geqslant \min(1, (P/\tau_1)^{-a}, \cdots, (P^k/\tau_k)^{-a}) \geqslant$$

$$\geqslant \min(1, P^{-\frac{1}{2}a}) = P^{-\frac{1}{2}a},$$

所以

$$H = H^{-a^2+\varepsilon} \cdot H^{1+a^2-\varepsilon} \leqslant$$

$$\leqslant H^{-a^2+\varepsilon} P^{(1+a^2-\varepsilon)(1-a)} \leqslant$$

$$\leqslant H^{-a^2+\varepsilon} P \cdot P^{-\frac{1}{2}a} \ll P H^{-a^2+\varepsilon} Z. \tag{4}$$

由 (2), (3) 及 (4) 可知：在 $\mathfrak{M}$ 上

$$S \ll P H^{-a^2+\varepsilon} Z. \tag{5}$$

4） 由 (2), (3) 及 (5) 式並簡單的不等式

$$||\xi|^{2t} - |\eta|^{2t}| \leqslant 2t|\xi-\eta|(|\xi|^{2t-1} + |\eta|^{2t+1}),$$

可知

$$|S|^{2t} - \left|B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)\right|^{2t} P^{2t}|R|^{2t} \ll H(PH^{-a^2+\varepsilon}Z)^{2t-1}.$$

在 $\mathfrak{M}\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)$ 上求積分，可得

$$K\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) = \left|B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)\right|^{2t} P^{2t} \int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}} \cdots \int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}} |R|^{2t} d\beta_1 \cdots d\beta_k +$$

$$+ O\left(HP^{2t-1} \cdot H^{-(2t-1)a^2+\varepsilon} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} Z^{2t-1} d\beta_1 \cdots d\beta_k\right).$$

由引理 10·2 可知

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} Z^{2t-1}\,d\beta_k\cdots d\beta_1 \leqslant P^{-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} Z^{2t-1}\,d\gamma_k\cdots d\gamma_1 \ll$$

$$\ll P^{-\frac{1}{2}k(k+1)}.$$

由此推出

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=$$

$$=\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\,d\beta_1\cdots d\beta_k+$$

$$+O\left(P^{2t-\frac{1}{2}k(k+1)-1}H^{1-a^2(2t-1)+\varepsilon}\right)$$

$$=\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t-\frac{k}{2}(k+1)}\int_{-q_k^{-1}\tau_k^{-1}P^k}^{q_k^{-1}\tau_k^{-1}P^k}\cdots\int_{-q_1^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P}|R|^{2t}\,d\gamma_1\cdots d\gamma_k+$$

$$+O\left(P^{2t-\frac{1}{2}k(k+1)-1}H^{1-a^2(2t-1)+\varepsilon}\right).\tag{6}$$

5) 易見

$$\left|\int_{-q_k^{-1}\tau_k^{-1}P^k}^{q_k^{-1}\tau_k^{-1}P^k}\cdots\int_{-q_1^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P}|R|^{2t}\,d\gamma_1\cdots d\gamma_k-\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|R|^{2t}\,d\gamma_1\cdots d\gamma_k\right|\ll$$

$$\ll \max_j M_j\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|R|^{2t-1}\,d\gamma_1\cdots d\gamma_k,$$

此處 M_j 是當 $|\gamma_j|>q_j^{-1}\tau_j^{-1}P^j$ 時 R 的極大值. 因

$$\frac{P^j}{\tau_j q_j}\geqslant\frac{P^j}{P^{\frac{1}{2}a-2\sigma}P^{j-\frac{1}{2}a+\sigma}}=P^{\sigma},\qquad 當\ 2\leqslant j\leqslant k,$$

及

$$\frac{P}{\tau_1 q_1}\geqslant\frac{P}{P^{\frac{1}{2}-\frac{1}{2}a+\sigma}P^{\frac{1}{2}}}=P^{\frac{1}{2}a-\sigma}\geqslant P^{\sigma},$$

故由引理 10·2

$$M_j\ll\max_{|\gamma_j|\geqslant P^{\sigma}}\delta_j^{-a^2}\ll P^{-a^2\sigma},$$

即得

$$\int_{-q_k^{-1}\tau_k^{-1}P^k}^{q_k^{-1}\tau_k^{-1}P^k}\cdots\int_{-q_1^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P}|R|^{2t}\,d\gamma_1\cdots d\gamma_k = c_1 + O(P^{-a^2\sigma}). \tag{7}$$

結合 (6), (7) 二式可知

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right) = c_1\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t-\frac12 k(k+1)} + $$
$$+ O(P^{2t-\frac12 k(k+1)-1}H^{1-a^2(2t-1)+\varepsilon}) + $$
$$+ O(P^{2t-\frac12 k(k+1)-a^2\sigma}H^{-2ta^2}). \tag{8}$$

命

$$A = \sum_{q_k\leqslant P^{\frac12 a-2\sigma}}\cdots\sum_{q_2\leqslant P^{\frac12 a-2\sigma}}\ \sum_{q_1\leqslant P^{\frac12-\frac12 a+\sigma}}\ \sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}.$$

由 (8) 可知

$$T_2 = c_1 A P^{2t-\frac12 k(k+1)} + O(P^{2t-\frac12 k(k+1)-1}\sum H^{1-a^2(2t-1)+\varepsilon}) + $$
$$+ O(P^{2t-\frac12 k(k+1)-a^2\sigma}\sum H^{-2ta^2}).$$

由於

$$\sum_q\sum_h H^{-2ta^2} \leqslant \sum_{q_1,\cdots,q_k} H^{1-2ta^2} \leqslant \left(\sum_{q=1}^{\infty} q^{1-2ta^2}\right)^k$$

的收斂性（因為 $t > k^2$）及當 $2t > 3k^2+1$ 時

$$\sum_q\sum_h H^{1-a^2(2t-1)+\varepsilon} \leqslant \left(\sum_q q^{2-a^2(2t-1)+\varepsilon}\right)^k$$

的收斂性，可知當 $2t > 3k^2+1$，

$$T_2 = c_1 A P^{2t-\frac12 k(k+1)} + O(P^{2t-\frac12 k(k+1)-c_4}). \tag{9}$$

假定 $2t > 3k^2 + 1$ 祇當 $k \geqslant 5$ 時成立．當 $k=3$ 及 4，我們須用以下的補充才能獲得 (9) 式：

當 $k=3$ 時，

$$\sum_q \sum_h H^{1-a^2(2t-1)+\varepsilon} =$$

$$= \sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{6}+\sigma}} \sum_{q_2 \leqslant P^{\frac{1}{6}-2\sigma}} \sum_{q_3 \leqslant P^{\frac{1}{6}-2\sigma}} (q_1 q_2 q_3)^{2-(18-1)/9+\varepsilon} \ll$$

$$\ll P^{(\frac{1}{3}+\sigma+\frac{1}{6}-2\sigma+\frac{1}{6}-2\sigma) \cdot 10/9+\varepsilon} \ll P^{\frac{20}{27}+\varepsilon};$$

及當 $k=4$ 時，

$$\sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{8}+\sigma}} q_1^{2-(48-1)/16+\varepsilon} \Big(\sum_{q \leqslant P^{\frac{1}{8}-2\sigma}} q^{2-(48-1)/16+\varepsilon} \Big)^3 \ll$$

$$\ll P^{-\frac{1}{16}\left(\frac{3}{8}+\frac{3}{8}\right)} \ll P^{\frac{3}{64}+\varepsilon}.$$

6) 今往求出 c_2 與 A 的差數．因為 $q_1, \cdots, q_k$ 的最小公倍數 $Q > \max(q_1, \cdots, q_k)$，所以

$$|c_2 - A| \leqslant F \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{h_1} \cdots \sum_{h_k} \left| B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \right|^{2t-1},$$

此處

$$F = \max_{Q \geqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma}} \left| B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \right|.$$

由引理 10·3 知道

$$F \ll Q^{-a+\varepsilon} \ll P^{-a(\frac{1}{2}-\frac{1}{2}a+\sigma)+\varepsilon}$$

及由同引理 $\sum_q \sum_h |B|^{2t-1}$ 是收斂的（因為 $2t > k(k+1)+1$），所以

$$c_2 = A + O(P^{-c_5}).$$

和（9）合併起來可知

$$T_{(2)} = c_1 c_2 P^{2t-\frac{1}{2}k(k+1)} + O\left(P^{2t-\frac{1}{2}k(k+1)-c_6}\right). \tag{10}$$

7）現在我們來討論 $T_{(1)}$. 若 $(\alpha_k, \cdots, \alpha_1)$ 屬於 E, 則必適合以下 k 個條件之一:

$$P^{\frac{1}{2}a-2\sigma} < q_\nu \leqslant P^{\nu-\frac{1}{2}a+\sigma}, \qquad 2 \leqslant \nu \leqslant k,$$

$$P^{\frac{1}{2}-\frac{1}{2}a+\sigma} < q_1 \leqslant P^{\frac{1}{2}}.$$

如果第一類不等式之一成立,卽有一 ν 使 $P^{\frac{1}{2}a-2\sigma} < q_\nu \leqslant P^{\nu-\frac{1}{2}a+\sigma}$, 則由引理 5·10 及 5·12 可知：當 $k > 9$ 及 $P \leqslant q_\nu$ 時,

$$S(\alpha_k, \cdots, \alpha_1) \ll P^{1-\lambda}, \qquad \lambda = \frac{1}{60\,k^3 \log k}; \tag{11}$$

而當 $P^{\frac{1}{2}a-2\sigma} < q_\nu$ 時,

$$S(\alpha_k, \cdots, \alpha_1) \ll P \cdot q^{-\frac{1}{k}+\varepsilon} \ll P^{1-\lambda}.$$

當 $k \leqslant 9$ 時, 由引理 5·10 及 5·11 也知此式眞實.

如果不適合第一類的不等式,則所討論的情况適合了引理 10·5 的假定,得出

$$S \ll P^{1-\sigma} \ll P^{1-\lambda}, \qquad \lambda = \frac{1}{60\,k^3 \log k}.$$

換言之,在 E 上常有（11）式.

8）現在我們將證明

$$T_{(1)} \ll P^{2t-\frac{1}{2}k(k+1)-c_7}. \tag{12}$$

8·1）假定 $k < 9$, 則由定理 5 及（11）式

$$T_{(1)} \ll P^{2(1-\lambda)} \int_0^1 \cdots \int_0^1 |S|^{2t-2}\, d\alpha_1 \cdots d\alpha_k \ll$$

$$\ll p^{2t-\frac{1}{2}k(k+1)-c_7}.$$

8·2) 今假定 $k \geqslant 9$，由定理 7 取 $t = t_1 + k^2$，則

$$T_{(1)} \ll \max_{\alpha \in E} |S|^{2k^2} \int_0^1 \cdots \int_0^1 |S|^{2t_1} d\alpha_1 \cdots d\alpha_k \ll$$

$$\ll p^{2k^2(1-\lambda)+2t_1-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)(1-a)^l} \ll$$

$$\ll p^{2t-\frac{1}{2}k(k+1)-c_5},$$

此處

$$c_5 = \frac{1}{30\,k\log k} - \frac{1}{2}k(k+1)(1-a)^l.$$

取

$$l = \left[\frac{\log(15\,k^2(k+1)\log k)}{-\log(1-a)}\right] + 1.$$

這保證了 $c_5 > 0$. 同時，當 $k \geqslant 9$ 時，

$$l < \frac{3\log k + \log\log k + \log(1+a) + \log 15}{-\log(1-a)} + 1 <$$

$$< k\,(3\log k + \log\log k + \log(1+a) + \log 15)\left(1 - \frac{1}{3}a\right) + 1,$$

所以

$$t = t_1 + k^2 \leqslant l\,k + \frac{1}{4}(k^2 + k + 2) + k^2 \leqslant$$

$$\leqslant k^2\,(3\log k + \log\log k + \log(1+a) + \log 15)\left(1 - \frac{1}{3}a\right) +$$

$$+ \frac{5}{4}(k^2 + k) + \frac{1}{2} <$$

$$< k^2\left(3\log k + \log\log k + \log\frac{10}{9} + \log 15 + \frac{5}{4}\right) -$$

$$- k\left(\log k - \frac{5}{4} - \frac{1}{2}a\right) <$$

$$< k^2(3\log k + \log\log k + 4) - 2.$$

由 (1), (10) 及 (12) 證出定理 16.

注意：我們並未算出定理 16 中 $k=2$ 的部份．讀者不難自己補出其證明．更進一步，在 $k=2$ 時，常數 c_1 及 c_2 都可能算出來．

§4. 定理 17 的敍述

定理 17. 命 k 表一 $\geqslant 2$ 的整數．s 是一 $\geqslant s_0$ 的整數，此處 s_0 的定義如次表：

k	2	3	4	5	6	7	8	$\geqslant 9$
s_0	7	19	49	127	315	763	1781	$2k^2(3\log k + \log\log k + 4)$

命 $I(N_k, \cdots, N_1)$ 代表下列方程組

$$\left.\begin{array}{l} p_1 + p_2 + \cdots + p_s = N_1, \\ p_1^2 + p_2^2 + \cdots + p_s^2 = N_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ p_1^k + p_2^k + \cdots + p_s^k = N_k \end{array}\right\} \quad (1)$$

的素數解 $p_1, \cdots, p_s$ 的組數．命 $N_k^{\frac{1}{k}} = P$．則 (1) 式的解組數可以表成

$$I(N_k, \cdots, N_1) = \frac{b_1 P^{s-\frac{1}{2}k(k+1)}\mathfrak{S}(N_k, \cdots, N_1)}{L^s} + O\left(\frac{P^{s-\frac{1}{2}k(k+1)}}{L^{s+1}}\log L\right),$$

此處

$$b_1 = \int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\,dx\right)^s e\left(-\frac{N_k}{P^k}\gamma_k - \cdots - \frac{N_1}{P}\gamma_1\right)d\gamma_k\cdots d\gamma_1,$$

$$\mathfrak{S}(N_k, \cdots, N_1) = \sum_{q_1, \cdots, q_k=1}^{\infty} A(q_k, \cdots, q_1),$$

$$A(q_k, \cdots, q_1) = \sum_{h_1, \cdots, h_k}{}' T^s e\left(-\frac{h_k}{q_k}N_k - \cdots - \frac{h_1}{q_1}N_1\right),$$

此處 $h_1,\cdots,h_k$ 分別經過一個既約剩餘系，mod $q_1,\cdots$, mod q_k，且

$$T=\frac{1}{\varphi(Q)}\sum_x{}' e\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right),$$

此處 Q 是 $q_1,\cdots,q_k$ 的最小公倍數，而 x 則經過一既約剩餘系，mod Q.

§5. 定理的證明

1) 命

$$S(\alpha_k,\cdots,\alpha_1)=\sum_{p\leqslant P}e(f(p)),\quad f(x)=\alpha_k x^k+\cdots+\alpha_1 x,$$

則

$$I(N_k,\cdots,N_1)=\int_0^1 d\alpha_1\cdots\int_0^1 S^s(\alpha_k,\cdots,\alpha_1)\,e(-N_k\alpha_k-\cdots-N_1\alpha_1)\,d\alpha_k=$$

$$=\int_{-\tau_1^{-1}}^{1-\tau_1^{-1}}d\alpha_1\cdots\int_{-\tau_k^{-1}}^{1-\tau_k^{-1}}S^s(\alpha_k,\cdots,\alpha_1)\,e(-N_k\alpha_k-\cdots-N_1\alpha_1)\,d\alpha_k,$$

此處 $\tau_\nu=P^\nu L^{-\sigma_\nu}$ 及

$$\sigma_\nu\geqslant 2^{6k+1}(\sigma_k+\cdots+\sigma_{\nu+1}+s_1+1),\quad \sigma_k>2k^2,$$

而 s_1 則是一任與的正整數.

對於 $(-\tau_\nu^{-1},1-\tau_\nu^{-1})$ 中的任意一個 α_ν，可有二整數 h_ν 及 q_ν 使

$$\alpha_\nu-\frac{h_\nu}{q_\nu}=\beta_\nu,\quad |\beta_\nu|\leqslant\frac{1}{q_\nu\tau_\nu},\quad (h_\nu,q_\nu)=1,\quad 0<q_\nu\leqslant\tau_\nu.$$

因之，所有的點 $(\alpha_k,\cdots,\alpha_1)$ 必定落在一個形如

$$\left|\alpha_\nu-\frac{h_\nu}{q_\nu}\right|\leqslant\frac{1}{q_\nu\tau_\nu},\quad 1\leqslant\nu\leqslant k,$$

的域內.

我們把所有這樣的域分爲下列幾類:

1°. 其中的 q_k 適合於 $L^{\sigma_k} \leqslant q_k \leqslant \tau_k$ 者, 用 $\mathfrak{m}_k$ 表示它們中間的一個;

2°. q_k 適合於 $0 < q_k < L^{\sigma_k}$ 及 q_{k-1} 適合於 $L^{\sigma_{k-1}} \leqslant q_{k-1} \leqslant \tau_{k-1}$ 者, 用 $\mathfrak{m}_{k-1}$ 表示它們中間的一個;

………………………………………………

ν°. 如果 $0 < q_k < L^{\sigma_k}, \cdots, 0 < q_{k-\nu+2} < L^{\sigma_{k-\nu+2}}$, 但 $L^{\sigma_{k-\nu+1}} \leqslant q_{k-\nu+1} \leqslant \leqslant \tau_{k-\nu+1}$, 則用 $\mathfrak{m}_{k-\nu+1}$ 表示它們中間的一個;

………………………………………………

k°. 如果 $0 < q_k < L^{\sigma_k}, \cdots, 0 < q_2 < L^{\sigma_2}$, 但 $L^{\sigma_1} < q_1 \leqslant \tau_1$, 則用 $\mathfrak{m}_1$ 表示它們中的一個;

$(k+1)$°. 適合於 $0 < q_\nu < L^{\sigma_\nu}$, $1 \leqslant \nu \leqslant k$ 的域用 $\mathfrak{M} = \mathfrak{M}\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)$ 來表它.

易於證明: 並無兩個 $\mathfrak{M}$ 有公共點. 用 $\mathfrak{N}$ 代表所有的 $\mathfrak{M}$ 之外的點的集合,則得

$$I(N_k, \cdots, N_1) = \left(\sum_{\mathfrak{M}} \int_{\mathfrak{M}} + \int_{\mathfrak{N}}\right) S^s e(-\alpha_k N_k - \cdots - \alpha_1 N_1)\, d\alpha_k \cdots d\alpha_1.$$

2) **引理 10·6.** 命

$$S^*(\beta_k, \cdots, \beta_1) = \int_2^P \frac{e(\Psi(x))}{\log x}\, dx, \quad \Psi(x) = \beta_k x^k + \cdots + \beta_1 x.$$

則在 $\mathfrak{M}\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)$ 上

$$S(\alpha_k, \cdots, \alpha_1) = T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \frac{1}{\varphi(Q)} S^*(\beta_k, \cdots, \beta_1) + O(P e^{-c_1\sqrt{L}}),$$

此處

$$T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) = \sum_{\substack{x=1 \\ (x,Q)=1}}^{Q} e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x\right),$$

而 Q 則是 $q_k, \cdots, q_1$ 的最小公倍數.

證：顯然有 $Q < L^{\sigma_1+\cdots+\sigma_k}$．命

$$S_m = \sum_{2\leqslant p\leqslant m} e\left(\frac{h_k}{q_k}p^k + \cdots + \frac{h_1}{q_1}p\right),\ S_1 = 0.$$

則由引理 7·14，

$$S_m = \sum_{\substack{x=1\\(x,Q)=1}}^{Q} e\left(\frac{h_k}{q_k}x^k + \cdots + \frac{h_1}{q_1}x\right)\sum_{\substack{p\leqslant m\\ p\equiv x(Q)}} 1 + O(Q^{\varepsilon}) =$$

$$= T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)\frac{\operatorname{li} m}{\varphi(Q)} + O(P e^{-c_2\sqrt{L}}).$$

我們有

$$S(\alpha_k, \cdots, \alpha_1) = \sum_{2\leqslant m\leqslant P}(S_m - S_{m-1})\, e(\Psi(m)) =$$

$$= \sum_{2\leqslant m\leqslant P} S_m\,(e(\Psi(m)) - e(\Psi(m+1))) + S_P\, e(\Psi(P+1)) =$$

$$= \frac{T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)}{\varphi(Q)}\Bigg(\sum_{2\leqslant m\leqslant P}\operatorname{li} m\,(e(\Psi(m)) - e(\Psi(m+1))) +$$

$$+ \operatorname{li} P\, e(\Psi(P+1))\Bigg) + O(P e^{-c_3\sqrt{L}}),$$

這是因為

$$P e^{-c_2\sqrt{L}}\left(\sum_{2\leqslant m\leqslant P}|\, e(\Psi(m)) - e(\Psi(m+1))\,| + 1\right) \ll$$

$$\ll P e^{-c_2\sqrt{L}} L^{\sigma_1+\sigma_2+\cdots+\sigma_k} \ll P e^{-c_3\sqrt{L}}.$$

又

$$\sum_{2\leqslant m\leqslant P}\operatorname{li} m\,(e(\Psi(m)) - e(\Psi(m+1))) + \operatorname{li} P\, e(\Psi(P+1)) =$$

$$= \sum_{3\leqslant m\leqslant P} e(\Psi(m))\int_{m-1}^{m}\frac{dx}{\log x} =$$

$$= \sum_{3\leqslant m\leqslant P} \int_{m-1}^{m} \frac{e(\Psi(x))}{\log x}\, dx + O(L^{\sigma_1+\cdots+\sigma_k}) =$$

$$= S^*(\beta_k, \cdots, \beta_1) + O(L^{\sigma_1+\cdots+\sigma_k}),$$

由此卽得出本引理.

引 理 10·7. 命 $\gamma_k, \cdots, \gamma_1$ 代表實數，$\Phi(y) = \gamma_k y^k + \cdots + \gamma_1 y$. 又命 $W = \prod_{\nu=1}^{k} \delta_\nu^{-a^2}$, $\delta_\nu = \max(1, \gamma_\nu)$, 則

$$\int_{2/P}^{1} \frac{e(\Phi(y))}{\log yP}\, dy = \frac{1}{L}\int_0^1 e(\Phi(y))\, dy + O\left(\frac{\log L}{L^2} W\right),$$

因而（引理 10·2）

$$\int_{2/P}^{1} \frac{e(\Phi(y))}{\log yP}\, dy \ll \frac{W}{L}.$$

證： 由第二中值定理及引理 10·2 可得

$$\frac{1}{L}\int_0^1 e(\Phi(y))\, dy - \int_{2/P}^{1} \frac{e(\Phi(y))}{\log yP}\, dy = \frac{1}{L}\int_0^{L^{-8}} e(\Phi(y))\, dy -$$

$$- \int_{2/P}^{L^{-8}} \frac{e(\Phi(y))}{\log y + L}\, dy + \frac{1}{L}\int_{L^{-8}}^{1} \frac{\log y}{\log y + L}\, e(\Phi(y))\, dy \ll$$

$$\ll L^{-8} \sum_{\nu=1}^{k} \max(1, L^{-8\nu} |\gamma_\nu|)^{-a^2} + \frac{\log L}{L^2} W \ll$$

$$\ll L^{-4(1-a)} W + \frac{\log L}{L^2} W \ll$$

$$\ll W L^{-2} \log L.$$

3) **引 理 10·8** 在 $\mathfrak{N}$ 上

$$S(\alpha_k, \cdots \alpha_1) \ll P L^{-\varepsilon_1}.$$

證：假定 α 在 $\mathfrak{m}_n$ 上，命

$$S_0=S\left(\frac{h_k}{q_k},\cdots,\frac{h_n}{q_n},\alpha_{n-1},\cdots,\alpha_1\right).$$

命 Q_n 代表 $q_k,\cdots,q_{n+1}$ 的最小公倍數．則 $Q_n\ll L^{\sigma_k+\cdots+\sigma_{n+1}}$．由定理 10，我們有

$$|S_0|\leqslant\sum_{t=1}^{Q_n}\Bigg|\sum_{\substack{p\leqslant P\\ p\equiv t(\bmod Q_n)}}e\left(\frac{h_n}{q_n}p^n+\cdots+\alpha_1 p\right)\ll$$

$$\ll PL^{-s_1-\sigma_k-\cdots-\sigma_{n+1}}.$$

(由於 $\sigma_n\geqslant 2^{6k+1}(\sigma_k+\cdots+\sigma_{n+1}+s_1+1)$.)

命

$$S(m)=\sum_{p\leqslant m}e\left(\frac{h_k}{q_k}p^k+\cdots+\frac{h_n}{q_n}p^n+\alpha_{n-1}p^{n-1}+\cdots+\alpha_1 p\right),$$

則得出

$$S(\alpha_k,\cdots,\alpha_1)=\sum_{m\leqslant P}(S(m)-S(m-1))\,e(\Psi(m))=$$

$$=\sum S(m)\,(e(\Psi(m))-e(\Psi(m+1))).$$

故得出

$$S(\alpha_k,\cdots,\alpha_1)\ll PL^{-s_1-\sigma_k-\cdots-\sigma_{n+1}}\sum_{m\leqslant P}(P^{-1}(L^{\sigma_k}+\cdots+L^{\sigma_{n+1}})+P^{-1})\ll$$

$$\ll PL^{-s_1}.$$

4) 當 $k\geqslant 3$，由定理 16 及引理 10·8 得出

$$\int\cdots\int_{\mathfrak{N}}|S(\alpha_k,\cdots,\alpha_1)|^s\,d\alpha_k\cdots d\alpha_1\ll(PL^{-s_1})^{s-s_0+1}\int\cdots\int_{\mathfrak{N}}|S(\alpha_k,\cdots,\alpha_1)|^{s_0-1}\,d\alpha_k\cdots d\alpha_1\ll$$

$$\ll P^{s-\frac{1}{2}k(k+1)}L^{-s_1}.$$

當 $k=2$，則由定理 5（定理 B_2），得出

$$\int\cdots\int_{\mathfrak{M}} |S(\alpha_3, \alpha_2, \alpha_1)|^7 \, d\alpha_3 \, d\alpha_2 \, d\alpha_1 \ll PL^{-s_1} \int_0^1\int_0^1\int_0^1 |S(\alpha_3, \alpha_2, \alpha_1)|^6 \, d\alpha_3 \, d\alpha_2 \, d\alpha_1 \ll$$

$$\ll P^{s-\frac{1}{2}k(k+1)} L^{-s_2+3}.$$

5) **引 理 10·9.** 若 $g \geqslant k^2+1$，則

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} |S^*(\beta_k, \cdots, \beta_1)|^g \, d\beta_k \cdots d\beta_1 \ll P^{g-\frac{1}{2}k(k+1)} L^{-g}.$$

證： 左邊的積分是

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} \left| \int_2^P \frac{e(\beta_k x^k + \cdots + \beta_1 x)}{\log x} \, dx \right|^g d\beta_k \cdots d\beta_1.$$

命 $x = Py$，$\beta_\nu = \gamma_\nu P^{-\nu}$，則此積分等於

$$P^{g-\frac{1}{2}k(k+1)} \int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} \left| \int_{2/P}^1 \frac{e(\gamma_k y^k + \cdots + \gamma_1 y)}{\log yP} \, dy \right|^g d\gamma_k \cdots d\gamma_1 \ll$$

$$\ll P^{g-\frac{1}{2}k(k+1)} L^{-g} \int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} W^g \, d\gamma_k \cdots d\gamma_1.$$

過程中用了引理 10·7. 由引理 10·2 即得出本引理.

引 理 10·10. 當 $s > k(k+1)$ 時，$\mathfrak{S}(N_k, \cdots, N_1)$ 絕對收斂.

證明 一如引理 10·3，但引用第一章推論 1·3 以代替定理 1.

6) 今仍利用簡單的不等式

$$|\xi^s - \eta^s| \leqslant s|\xi - \eta|(|\xi|^{s-1} + |\eta|^{s-1}).$$

由引理 10·6 得出

$$\sum_{\mathfrak{M}} \int\cdots\int_{\mathfrak{M}} S^s(\alpha_k, \cdots, \alpha_1) \, e(-N_k\alpha_k - \cdots - N_1\alpha_1) \, d\alpha_k \cdots d\alpha_1 -$$

$$-\sum_{\mathfrak{M}} \left(\frac{T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)}{\varphi(Q)} \right)^s e\left(-\frac{N_k h_k}{q_k} - \cdots - \frac{N_1 h_1}{q_1} \right) \times$$

$$\times \int\cdots\int_{\mathfrak{M}} S^{*s}(\beta_k,\cdots,\beta_1)\, e(-N_k\beta_k-\cdots-N_1\beta_1)\, d\beta_k\cdots d\beta_1 \ll$$

$$\ll P e^{-c_1\sqrt{L}}\Big(\int_0^1\cdots\int_0^1 |S(\alpha_k,\cdots,\alpha_1)|^{s-1}\, d\alpha_k\cdots d\alpha_1 +$$

$$+\sum_q\sum_h Q^{-(s-1)a+\varepsilon}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} |S^*(\beta_k,\cdots,\beta_1)|^{s-1}\, d\beta_k\cdots d\beta_1\Big) \ll$$

$$\ll P^{s-\frac{1}{2}k(k+1)} e^{-c_1\sqrt{L}}.$$

在獲得此式的過程中我們根據了以下的一些事實：由定理 15 有

$$\int_0^1\cdots\int_0^1 |S(\alpha_k,\cdots,\alpha_1)|^{s-1}\, d\alpha_k\cdots d\alpha_1 \ll P^{s-1-\frac{1}{2}k(k+1)}.$$

（當 $k=2$ 時需略加修正，但這種修正並不困難）．又由引理 10·9，

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} |S^*|^{s-1}\, d\beta_k\cdots d\beta_1 \ll P^{s-1-\frac{1}{2}k(k+1)}$$

及

$$\sum_q\sum_h Q^{-(s-1)a+\varepsilon} \leqslant \sum_q (q_1\cdots q_k)^{1-(s-1)a^2+\varepsilon} = O(L^{c_5}).$$

（因為 $q_1,\cdots,q_k$ 的最小公倍數 $\geqslant (q_1\cdots q_k)^a$.）

7）我們有

$$\Big(\sum_{\mathfrak{M}} - \sum_{q_k\leqslant L^{\frac{1}{2}\sigma_k}}\cdots\sum_{q_1\leqslant L^{\frac{1}{2}\sigma_1}}\sum_{h_1}{}'\cdots\sum_{h_k}{}'\Big)\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{N_k h_k}{q_k}-\cdots-\frac{N_1 h_1}{q_1}\right)\times$$

$$\times\int\cdots\int_{\mathfrak{M}} S^{*s} e(-N_k\beta_k-\cdots-N_1\beta_1)\, d\beta_k\cdots d\beta_1 \ll$$

$$\ll M\sum_{q_k=1}^{\infty}\cdots\sum_{q_1=1}^{\infty}\sum_{h_1}{}'\cdots\sum_{h_k}{}'\left|\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right|^{s-1}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|S^*|^s\, d\beta_k\cdots d\beta_1, \quad (2)$$

此處

$$M=\max_{\nu}\max_{q_\nu\geqslant L^{\frac{1}{2}\sigma_\nu}}\left|\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right|.$$

由第一章推理 1·3 已知

$$M\ll\max_{\nu}\max_{q_\nu\geqslant L^{\frac{1}{2}\sigma_\nu}}Q^{-a+\varepsilon}\ll\max_{\nu}\max_{q_\nu\geqslant L^{\frac{1}{2}\sigma_\nu}}q_\nu^{-a+\varepsilon}\ll$$

$$\ll L^{-a\sigma_k+\varepsilon}\ll L^{-1},$$

及由引理 10·10, (2) 式中的級數是收斂的; 再由引理 10·9, (2) 式中的積分部份是 $\ll P^{s-\frac{1}{2}k(k+1)}L^{-s}$. 故知 (2) 式之右邊 $\ll P^{s-\frac{1}{2}k(k+1)}L^{-s-1}$.

8) 當 $q_\nu\leqslant L^{\frac{1}{2}\sigma_\nu}$, $1\leqslant\nu\leqslant k$, 我們有

$$\left(\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}-\int_{\mathfrak{M}}\cdots\int\right)|S^*|^s\,d\beta_1\cdots d\beta_k\ll$$

$$\ll M\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|S^*|^{s-1}\,d\beta_1\cdots d\beta_k, \tag{3}$$

此處

$$M=\max_{\nu}\max_{|\beta_\nu|>q_\nu^{-1}P^{-\nu}L^{\sigma_\nu}}|S^*|.$$

由引理 10·7 及

$$|\gamma_\nu|=P^\nu|\beta_\nu|>q_\nu^{-1}L^{\sigma_\nu}\geqslant L^{\frac{1}{2}\sigma_\nu},$$

可知

$$M\ll\frac{P}{L}\max_{\nu}\max_{|\gamma_\nu|>L^{\frac{1}{2}\sigma_\nu}}\min(1,|\gamma_\nu|^{-a^2})\ll\frac{P}{L}L^{-\frac{1}{2}a^2\sigma_k}\ll PL^{-2}.$$

再用引理 10·9, (3) 式的右邊 $\ll P^{s-\frac{1}{2}k(k+1)}L^{-s-1}$. 聯合 (2) 及 (3), 可以得到

$$\sum_{\mathfrak{M}}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right)\int_{\mathfrak{M}}\cdots\int S^{*s}(\beta_k,\cdots,\beta_1)\times$$

$$\times e(-N_k\beta_k-\cdots-N_1\beta_1)\,d\beta_k\cdots d\beta_1=$$

$$=\sum_{q_k\leqslant L^{\frac{1}{2}\sigma_k}}\cdots\sum_{q_1\leqslant L^{\frac{1}{2}\sigma_1}}\sum_{h_k}\cdots\sum_{h_1}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right)\times$$

$$\times\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}S^{*s}(\beta_k,\cdots,\beta_1)\,e(-\beta_k N_k-\cdots-\beta_1 N_1)\,d\beta_k\cdots d\beta_1+$$

$$+O\left(P^{s-\frac{1}{2}k(k+1)}L^{-s-1}\right). \tag{4}$$

9) 當 $k\geqslant 3$，我們有

$$\mathfrak{S}(N_k,\cdots,N_1)-\sum_{q_k\leqslant L^{\frac{1}{2}\sigma_k}}\cdots\sum_{q_1\leqslant L^{\frac{1}{2}\sigma_1}}\sum_{h_k}\cdots\sum_{h_1}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s\times$$

$$\times e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right)\ll$$

$$\ll M\sum_{q_k=1}^{\infty}\cdots\sum_{q_1=1}^{\infty}\sum_{h_1}{}'\cdots\sum_{h_k}{}'\left|\frac{1}{\varphi(Q)}T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{s-1}, \tag{5}$$

此處
$$M=\max_{\nu}\max_{q_\nu\geqslant L^{\frac{1}{2}\sigma_\nu}}\left|\frac{1}{\varphi(Q)}T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|.$$

由 $M\ll L^{-\frac{1}{2}a\sigma_k+\varepsilon}\ll L^{-1}$ 及引理 10·10，所以 (5) 式的右邊 $\ll L^{-1}$．（當 $k=2$，須加修改）．

因此得出

$$\sum_{\mathfrak{M}}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{h_k N_k}{q_k}-\cdots-\frac{h_1 N_1}{q_1}\right)\times$$

$$\times\int\cdots\int_{\mathfrak{M}}S^{*s}e(-N_k\beta_k-\cdots-N_1\beta_1)\,d\beta_k\cdots d\beta_1=$$

$$=\mathfrak{S}(N_k,\cdots,N_1)\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}S^{*s}(\beta_k,\cdots,\beta_1)\,e(-\beta_k N_k-\cdots-\beta_1 N_1)\,d\beta_k\cdots d\beta_1+$$

$$+O\left(P^{s-\frac{1}{2}k(k+1)}L^{-s-1}\right).$$

10) 我們有

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} S^{*s}(\beta_k,\cdots,\beta_1)\, e(-N_k\beta_k-\cdots-N_1\beta_1)\, d\beta_k\cdots d\beta_1=$$

$$=P^{s-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{2/P}^{1}\frac{e(\gamma_k x^k+\cdots+\gamma_1 x)}{\log xP}\,dx\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)d\gamma_k\cdots d\gamma_1.$$

由引理 10·7,

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{2/P}^{1}\frac{e(\gamma_k x^k+\cdots+\gamma_1 x)}{\log xP}\,dx\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)d\gamma_k\cdots d\gamma_1=$$

$$=\frac{1}{L^s}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{0}^{1}e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)d\gamma_k\cdots d\gamma_1+$$

$$+O\left(\frac{\log L}{L^{s+1}}\right)\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}W^{s-1}\,d\gamma_k\cdots d\gamma_1=\frac{b_1}{L^s}+O\left(\frac{\log L}{L^{s+1}}\right).$$

所以最後獲得

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}} S^s(\alpha_k,\cdots,\alpha_1)\, e(-\alpha_k N_k-\cdots-\alpha_1 N_1)\, d\alpha_k\cdots d\alpha_1=$$

$$=b_1\,\mathfrak{S}(N_k,\cdots N_1)\frac{P^{s-\frac{1}{2}k(k+1)}}{L^s}+O\left(\frac{P^{s-\frac{1}{2}k(k+1)}}{L^{s+1}}\log L\right),$$

此處

$$b_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{0}^{1}e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)d\gamma_k\cdots d\gamma_1.$$

因此得出本引理.

如果 $b_1\geqslant b>0$ 及 $\mathfrak{S}(N_k,\cdots,N_1)\geqslant c>0$ (此處 b 及 c 與 N 無關), 則可以得出: 當 N 充分大時, 不定方程

$$\sum_{\nu=1}^{s}p_\nu^h=N_h,\qquad 1\leqslant h\leqslant k,$$

有素數解 $p_1,\cdots,p_s$. 保證 $b_1\geqslant b>0$ 的條件將稱為 "正可解條件", 而保證 $c_1\geqslant c>0$ 的條件則稱為 "相合可解條件".

§6. 附　　錄

在本章的開始就已說明：爲了避免煩瑣起見把 $k=2$ 的情况除外．由以上的方法略加修改，我們不難獲得本章定理對 $k=2$ 時的眞實性．不但如此，在本節中我們還進一步具體地算出正可解條件的積分，和相合可解條件的奇異級數．爲了不太冗長，我們將略去許多複雜的計算．

1）正可解條件的研究．

在計算中我們要用到下面幾個結果：

1°．命 $\delta>0$，$\alpha>0$．有不等式

$$(\delta-x_1-\cdots-x_n)^2+\alpha(x_1^2+\cdots+x_n^2)\geq\frac{\alpha}{n+\alpha}\delta^2. \tag{1}$$

等號僅當 $x_1=\cdots=x_n=\frac{\delta}{n+\alpha}$ 時成立．

2°．命 $a<0$ 及 $b>0$．又命 $f(x)$ 是一 (a,b) 中的連續函數．則

$$\lim_{\omega\to\infty}\int_a^b\frac{\sin 2\pi x\omega}{\pi x}f(x)\,dx=f(0). \tag{2}$$

3°．命 $Q(x_1,\cdots,x_n)=\sum_{i,j=1}^{n}q_{ij}x_ix_j$ 代表一定正二次型，它的行列式用 $|Q|$ 代表它．又 $L(x_1,\cdots,x_n)$ 是一齊次線性式，同時 L 也表示其係數所成的矢量．又命 $A>0$．命 R 表一超橢圓體的內部：

$$A+2L(x_1,\cdots,x_n)-Q(x_1,\cdots,x_n)>0.$$

方陣

$$\begin{pmatrix} A & L \\ L' & -Q \end{pmatrix}$$

的行列式的絕對值以 $|\Delta|$ 表它．L' 表由 L 的係數自上而下排成的列．則

$$\int_R \cdots \int \frac{dx_1 \cdots dx_n}{\sqrt{A+2L(x_1,\cdots,x_n)-Q(x_1,\cdots,x_n)}} = |Q|^{-\frac{1}{2}n} |\Delta|^{\frac{1}{2}(n-1)} \frac{\pi^{\frac{1}{2}(n+1)}}{\Gamma(\frac{1}{2}(n+1))} . \quad (3)$$

4°. 命 Δ_n 是二次型 $(x_1+\cdots+x_n)^2+2x_1^2+\cdots+2x_n^2$ 的行列式，則 $\Delta_n=(n+2)\,2^{n-1}$. 又命 U 是二次型

$$u\,x_0^2+2v\,x_0(x_1+\cdots+x_n)+(x_1+\cdots+x_n)^2+2\,x_1^2+\cdots+2\,x_n^2$$

的行列式，則

$$U=2^{n-1}\left((n+2)(u+v^2)-2(n+1)\,v^2\right).$$

現在研究與正可解有關的定積分

$$J(\delta)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left(\int_0^1 e^{2\pi i(\alpha_2 x^2+\alpha_1 x)}\,dx\right)^s e^{-2\pi i(\alpha_2+\alpha_1\delta)}\,d\alpha_2\,d\alpha_1 .$$

把它當做

$$J_\omega(\delta)=\int_{-\omega}^{\omega}\int_{-\omega}^{\omega}\left(\int_0^1 e^{2\pi i(\alpha_2 x^2+\alpha_1 x)}\,dx\right)^s e^{-2\pi i(\alpha_2+\alpha_1\delta)}\,d\alpha_2\,d\alpha_1$$

的極限． 命

$$X=x_1^2+\cdots+x_s^2-1, \qquad Y=x_1+\cdots+x_s-\delta,$$

則

$$J_\omega(\delta)=\int_0^1\cdots\int_0^1 \frac{\sin 2\pi X\omega}{\pi X}\,\frac{\sin 2\pi Y\omega}{\pi Y}\,dx_1\cdots dx_s=$$

$$=2\int_{\substack{0\\x_1\geqslant x_2}}^1\cdots\int_0^1 \frac{\sin 2\pi X\omega}{\pi X}\,\frac{\sin 2\pi Y\omega}{\pi Y}\,dx_1\cdots dx_s .$$

現有

$$J_\omega(\delta)=\int\int \frac{\sin 2\pi X\omega}{\pi X}\,\frac{\sin 2\pi Y\omega}{\pi Y}\,dX\,dY\int_0^1\cdots\int_0^1 \frac{dx_3\cdots dx_s}{x_1-x_2} .$$

由 2° 可得

$$J(\delta)=\lim_{\omega\to\infty}J_\omega(\delta)=\underset{\substack{x_1^2+\cdots+x_s^2=1\\ x_1+\cdots+x_s=\delta\\ x_1>x_2}}{\int\cdots\int}\frac{dx_3\cdots dx_s}{x_1-x_2}=$$

$$=\int\underset{\mathfrak{D}}{\cdots}\int\frac{dx_3\cdots dx_s}{\sqrt{2(1-x_3^2-\cdots-x_s^2)-(\delta-x_3-\cdots-x_s)^2}}.$$

這積分所經過的範圍 $\mathfrak{D}$ 受下列一些條件的限制:

$$2(1-x_3^2-\cdots-x_s^2)\geqslant(\delta-x_3-\cdots-x_s)^2, \tag{4}$$

$$(\delta-x_3-\cdots-x_s)^2\geqslant 1-x_3^2-\cdots-x_s^2, \tag{5}$$

$$x_\nu\geqslant 0. \tag{6}$$

由 1° 可知 $(\delta-x_3-\cdots-x_s)^2+2(x_3^2+\cdots+x_s^2)\geqslant 2\delta^2/s$. 根據此式可知: 若 $s<\delta^2$, 則 (4) 式決不可能; 即當 $s<\delta^2$ 時, $J(\delta)=0$. 又由 (6) 式,我們可以看出,在積分範圍內 $x_3+\cdots+x_s\leqslant\delta$. 若 $\delta<1$, 則由

$$1-x_3^2-\cdots-x_s^2\geqslant 1-(x_3+\cdots+x_s)^2\geqslant(1-x_3-\cdots-x_s)^2\geqslant(\delta-x_3-\cdots-x_s)^2,$$

(5) 式成為不可能. 因之當 $\delta\leqslant 1$ 時,$J(\delta)=0$.

今假定 $s>\delta^2$. (4) 表示在超橢圓體 $2(1-x_3^2-\cdots-x_s^2)=(\delta-x_3-\cdots-x_s)^2$ 之內,而 (5) 表示在超橢圓體 $1-x_3^2-\cdots-x_s^2=(\delta-x_3-\cdots-x_s)^2$ 之外. 又易見凡第一個超橢圓體上之點一定在第二個超橢圓體之外,而第二個超橢圓體上之點一定在第一個超橢圓體之內. 換言之,第一個超橢圓體一定包有第二個超橢圓體. 這兩超橢圓體的共同部份 $x_3+\cdots+x_s=\delta$, $x_3^2+\cdots+x_s^2=1$ 是一低於 $s-2$ 維的域,所以有一塊有正 n 維容積的部份存在適合 (4), (5) 及 (6). 即得

引理 10·11. 命 $s>3$. 若 $s>\delta^2>1$, 則 $J(\delta)>0$.

如果我們更假定 $\delta^2 > s-1$，則我們還可以算出函數 $J(\delta)$．因為不等式 (5) 可以取消：卽當 $\delta^2 > s-1$，則由 1°，可知

$$x_3^2 + \cdots + x_s^2 + (\delta - x_3 - \cdots - x_s)^2 \geqslant \frac{1}{s-1}\delta^2 > 1,$$

卽 (5) 自然地適合了．

又 (6) 式也可以取消：由 (4) 已知 $x_\nu \leqslant 1$，如果 $x_3 + \cdots + x_s < 0$，則

$$(\delta - x_3 - \cdots - x_s)^2 \geqslant \delta^2 \geqslant s-1 \geqslant 2,$$

這是和 (4) 式相矛盾的．所以 $x_3, \cdots, x_s$ 中至少有一個是正的．假定其中還有一個是負的．我們可以假定 $x_3 \geqslant 0$，$x_4 < 0$，則

$$(\delta - (x_3 + x_4) - x_5 - \cdots - x_s)^2 + 2(x_3^2 + \cdots + x_s^2) >$$

$$> (\delta - (x_3 + x_4) - x_5 - \cdots - x_s)^2 + 2((x_3 + x_4)^2 + x_5^2 + \cdots + x_s^2) \geqslant$$

$$\geqslant \frac{2}{s-1}\delta^2 \geqslant 2$$

(由 1°)．這和 (4) 式相違背．所以由 (4) 式可以自然地推出 (5) 及 (6)．故得

$$J(\delta) = \underset{(\delta - x_3 - \cdots - x_s)^2 < 2(1 - x_3^2 - \cdots - x_s^2)}{\int \cdots \int} \frac{dx_3 \cdots dx_s}{\sqrt{2(1 - x_3^2 - \cdots - x_s^2) - (\delta - x_3 - \cdots - x_s)^2}}$$

在 3° 中取 $n = s-2$，$A = 2 - \delta^2$，$L(x_1, \cdots, x_n) = \delta(x_3 + \cdots + x_s)$ 及 $Q(x_3, \cdots, x_s) = (x_3 + \cdots + x_s)^2 + 2(x_3^2 + \cdots + x_s^2)$．則由 4° 可知

$$|Q| = s \cdot 2^{s-3}, \quad |\Delta| = 2^{s-2}(s - \delta^2).$$

所以由 3° 得出

引 理 10·12. 若 $s \geqslant 3$ 及 $s \geqslant \delta^2 \geqslant s-1$, 則

$$J(\delta) = s^{1-\frac{1}{2}s}(s-\delta^2)^{\frac{1}{2}(s-3)} \frac{\pi^{\frac{1}{2}(s-1)}}{\Gamma(\frac{1}{2}(s-1))}.$$

2) 相合可解條件的研究.

關於 $\mathfrak{S}(N_2, N_1)$ 的算出,更爲煩雜. 我們現在僅大概說明其計算方法,並敍述其重要結論如次:

我們改寫

$$T\left(\frac{u}{p^l}, \frac{v}{p^l}\right) = T(u, v, p^l), \qquad (u, v) = 1.$$

用

$$S(u, p^l) = \sum_{x=1}^{p^l} e_{p^l}(u x^2)$$

代表普通的 Gauss 和. 關於此和的數值我們熟知有以下的結果:

1°.
$$S(u, p^l) = \left(\frac{u}{p}\right)^l S(1, p^l) \qquad 若 p > 2, \tag{7}$$

$$S(u, 2^l) = (-1)^{\frac{1}{8}(u^2-1)l}\, i^{-\frac{1}{4}(u-1)^2} S(1, 2^l), \tag{8}$$

$$S(1, p^l) = i^{\frac{1}{4}(p^l-1)^2} p^{\frac{1}{2}l} \qquad 若 p > 2, \tag{9}$$

$$S(1, 2^l) = \begin{cases} 0 & 若 l = 1, \\ (1+i)\, 2^{\frac{1}{2}l} & 若 l > 1. \end{cases} \tag{10}$$

2°. 我們引進整數 γ、其定義是

$$p^\gamma \| (2u, v).$$

於是我們有以下的

引 理 10·13. 假定 $l > 2\gamma + 1$. 若相合式

$$2ux + v \equiv 0 \pmod{p^{\gamma+1}}, \quad p \nmid x \tag{11}$$

無解,則

$$T(u, v, p^l) = 0. \tag{12}$$

若不然，命 x_0 是

$$2ux + v \equiv 0 \pmod{p^{l+\gamma}} \tag{13}$$

的解，則

$$T(u, v, p^l) = e_{p^l}(-u x_0^2)\ S(u, p^l) = e_{p^l}(-v^2/(4u))\ S(u, p^l), \tag{14}$$

此處 $v^2/4u$ 和 $u x_0^2$ 是一對模 p^l 的整數.

證：命 $x = y + p^{l-\gamma-1}z$，則

$$T(u, v, p^l) = \sum_{y, p^{l-\gamma-1}}^{*} e_{p^l}(uy^2 + vy) \sum_{z, p^{\gamma+1}} e_{p^l}((2uy + v)\, p^{l-\gamma-1} z) =$$

$$= p^{\gamma+1} \sum_{\substack{y, p^{l-\gamma-1} \\ 2uy+v\equiv 0 \pmod{p^{\gamma+1}}}} e_{p^l}(uy^2 + vy),$$

此處 $\sum\limits_{y, p^l}$ 代表一和，y 經過一剩餘系，mod p^l；$\sum\limits_{y, p^l}^{*}$ 代表一和，y 經過一既約剩餘系，mod p^l.

顯然當（11）無解時，此和爲零. 不然命 x_0 是適合（13）的解. 則（11）式所有的解可以表成

$$x = x_0 + py, \qquad 1 \leqslant y \leqslant p^{l-1}.$$

以此代入原和，卽得

$$T(u, v, p^l) = \sum_{y, p^{l-1}} e_{p^l}(u(x_0 + py)^2 + v(x_0 + py)) =$$

$$= e_{p^l}(ux_0^2 + vx_0) \sum_{y, p^{l-1}} e_{p^{l-2}}(uy^2) =$$

$$= e_{p^l}\left(-\frac{v^2}{4u}\right) p\, S(u, p^{l-2}) =$$

$$= e_{p^l}\left(-\frac{v^2}{4u}\right) S(u, p^l).$$

3°. 當 $l \leqslant 2\gamma+1$ 時，$T(u,v,p^l)$ 可以一一算出；特別是 $p>2$，則 $\gamma=0$，而有

$$T(u,v,p)=\sum_{x,p} e(ux^2+vx)-1= \\ =\begin{cases} e_p\left(-\frac{v^2}{4u}\right)S(u,p)-1 & \text{若 } p\nmid u, \\ -1 & \text{若 } p\mid u. \end{cases} \tag{15}$$

當 $p=2$ 時，$l\leqslant 3$，直接可以算出

$$\left.\begin{aligned} &T(u,v,2)=(-1)^{u+v}, \\ &T(u,v,4)=i^{u+v}(1+(-1)^v), \\ &T(u,v,8)=\left(\frac{1+i}{\sqrt{2}}\right)^{u+v}(1+i^v)(1+(-1)^v). \end{aligned}\right\} \tag{16}$$

至此，我們已經有了足夠的方法來算出 $T(u,v,p^l)$ 的數值.

4°. 命

$$A(p^l)=\sum_{\substack{u=1 \\ p\nmid(u,v)}}^{p^l}\sum_{v=1}^{p^l}\left(\frac{T(u,v,p^l)}{\varphi(p^l)}\right)e_{p^l}(-N_2u-N_1v).$$

經冗長之計算後可以得出以下的二引理.

引理 10·14. 假定 $l>1$. 當 p^l 充分大時，

$$A(p^l)=0.$$

（在證明此引理時，將用到 $sN_2-N_1^2\neq 0$，而此點為正可解條件 $N_1^2<sN_2$ 所保證）.

引理 10·15.

$$A(p)\ll p^{1-\frac{1}{2}s}.$$

命

$$\vartheta_p=\sum_{l=0}^{\infty}A(p^l).$$

由引理 10·14 可知 ∂_p 僅是一個有限的級數．並且當 p 充分大時，

$$\partial_p = 1 + A(p).$$

再由引理 10·15 可知：當 $s \geqslant 5$ 時，

$$\prod_p \partial_p$$

是一絕對收斂的無窮乘積．由此可知

引理 10·16． 當 $s \geqslant 5$ 時，

$$\mathfrak{S}(N_2, N_1) = \prod_p \partial_p$$

是一絕對收斂的級數．

5°．更複雜的計算可以證明：

當 $s \geqslant 5$ 及 $p \geqslant 5$ 時，$\partial_p > 0$；又若 $2 \mid s - N_1$ 及 $8 \mid s - N_2$ 時，$\partial_2 > 0$；而若 $3 \mid s - N_2$ 時，$\partial_3 > 0$．總之，可以證明

引理 10·17． 命 $s \geqslant 5$．若 $2 \mid s - N_1$ 及 $24 \mid s - N_2$，則

$$\mathfrak{S}(N_2, N_1) > 0.$$

把本節的結果和定理 17 聯合起來，可以得出以下的更明確的結論：

命 $N_1(t)$，$N_2(t)$ 是兩組正整數隨 t 趨向無窮．假定

$$1 < \varlimsup_{t \to \infty} \frac{N_1^2(t)}{N_2(t)} < 7.$$

並假定 $N_1(t)$ 是奇數，$N_2(t) \equiv 7 \pmod{24}$，則當 t 充分大時，有七個素數 $p_1, \cdots, p_7$ 使

$$p_1^2 + \cdots + p_7^2 = N_2,$$

$$p_1 + \cdots + p_7 = N_1.$$

第十一章

前章問題進一步的研究

§ 1.

本章中將闡明"正可解條件"及"相合可解條件"的含義並將給與一些條件來保證"正可解"及"相合可解". 因之,在這些條件之下,及當 $s>2k^2(3\log k+$ $+\log\log k+4)$ 及 N 充分大時,方程組

$$p_1^k+\cdots+p_s^k=N_k,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$p_1+\cdots+p_s=N_1,$$

有素數解.

本章的另一目的在縮小 s 的限制. 換言之,我們將把 s 所大於的數減低成爲

$$2k^2+3+k\log(60k^3\log k)\Big/\log\frac{1}{1-a}\sim 3k^2\log k,$$

卽當 s 大於上數及充分大的 $N_k,\cdots,N_1$ 適合"正可解"及"相合可解"的條件時,上方程組有解答.

§ 2. 正可解條件的研究

命

$$b_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx\right)^s e(-\gamma_k\delta_k-\gamma_{k-1}\delta_{k-1}-$$

$$-\cdots-\gamma_1\delta_1)\,d\gamma_k\cdots d\gamma_1.$$

命

$$B(\omega_k,\cdots,\omega_1)=\int_{-\omega_k}^{\omega_k}d\gamma_k\cdots$$

$$\cdots\int_{-\omega_1}^{\omega_1}\left(\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx\right)^s e(-\gamma_k\delta_k-\gamma_{k-1}\delta_{k-1}-\cdots-\gamma_1\delta_1)\,d\gamma_1.$$

如是，由定義

$$b_1=\lim_{\omega_k\to\infty}\cdots\lim_{\omega_1\to\infty}B(\omega_k,\cdots,\omega_1).$$

交換積分號，可得

$$B(\omega)=B(\omega_k,\cdots,\omega_1)=\int_0^1\cdots\int_0^1 dx_1\cdots dx_s\times$$

$$\times\int_{-\omega_k}^{\omega_k}\cdots\int_{-\omega_1}^{\omega_1}e(\gamma_k(x_1^k+\cdots+x_s^k-\delta_k)+\cdots+\gamma_1(x_1+\cdots+x_s-\delta_1))\,d\gamma_k\cdots d\gamma_1=$$

$$=\int_0^1\cdots\int_0^1\frac{\sin 2\pi\omega_k(x_1^k+\cdots+x_s^k-\delta_k)}{x_1^k+\cdots+x_s^k-\delta_k}\cdots\frac{\sin 2\pi\omega_1(x_1+\cdots+x_s-\delta_1)}{x_1+\cdots+x_s-\delta_1}\,dx_1\cdots dx_s.$$

命

$$\left.\begin{array}{l}X_1=x_1+\cdots+x_s-\delta_1\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ X_k=x_1^k+\cdots+x_s^k-\delta_k\end{array}\right\},$$

則函數行列式

$$J=\frac{D(x_1,\cdots,x_k)}{D(X_1,\cdots,X_k)}=\frac{1}{k!}\begin{vmatrix}1,&\cdots,&1\\ x_1,&\cdots,&x_k\\ \cdots&\cdots&\cdots\\ x_1^{k-1},&\cdots,&x_k^{k-1}\end{vmatrix}^{-1}=\frac{1}{k!\prod\limits_{k\geq i>j\geq 1}(x_i-x_j)}.$$

把 k 維單位方體分成若干份 D_i，在每一份中 J 都不變號．如此則得

$$B(\omega)=\sum_{j}\int\underset{D_j}{\cdots}\int\frac{\sin 2\pi\omega_1 X_1}{X_1}\cdots\frac{\sin 2\pi\omega_k X_k}{X_k}\,dX_1\cdots dX_k\times$$

$$\times\underset{\substack{0\leqslant x_1\leqslant 1\\ \cdots\\ 0\leqslant x_k\leqslant 1}}{\int_0^1\cdots\int_0^1}\frac{dx_{k+1}\cdots dx_s}{k!\prod(x_i-x_j)}.$$

由 Dirichlet 定理可知：如果方程組

$$X_\mu=x_1^\mu+\cdots+x_s^\mu-\delta_\mu=0,\qquad x_\nu\leqslant 1,\quad 1\leqslant\mu\leqslant k,\tag{2}$$

有正數解答，則

$$\lim_{\omega\to\infty}B(\omega)=\underset{\substack{0\leqslant x_\nu\leqslant 1\\ X_\nu=0}}{\int_0^1\cdots\int_0^1}\frac{dx_{k+1}\cdots dx_s}{k!\left|\prod(x_i-x_j)\right|}>0.\tag{3}$$

所以我們一變而爲求

$$x_1^\mu+\cdots+x_s^\mu=\delta_\mu,\quad 0\leqslant x_\nu\leqslant 1,\quad 1\leqslant\mu\leqslant k,\quad 1\leqslant\nu\leqslant s,$$

有正數解答的問題． 用 $\delta_\mu=N_\mu/P^\mu$ 代入，也就是

$$Z_1^\mu+\cdots+Z_s^\mu=N_\mu,\qquad 1\leqslant\mu\leqslant k,\tag{4}$$

有無正數解答的問題． 這一條件十分自然，因爲如果連正數的解答都沒有，還談什麼有正整數解的問題，更勿論有素數解的問題． 尚須注意者，因爲 $N_k^a=P$，所以 $\delta_k=1$，因之 $x_\nu\leqslant 1$ 也是自然的結果，而不必另添假定了．

所以"正可解條件"就是保證 (4) 式有正數解答的條件，這是命名的來由．

引理 11·1. 方程組

$$x_1^h+\cdots+x_k^h=\delta_h,\qquad 1\leqslant h\leqslant k,\tag{5}$$

有正數解，且 $x_i \neq x_j$ $(i \neq j)$，的條件是二次型

$$\sum_{i,j=1}^{k} \delta_{i+j-1} t_i t_j \tag{6}$$

是定正的，此處 $\delta_v(v > k)$ 可由次式巡迴定義之：

$$\begin{vmatrix} \delta_1, & 1, & 0, & \cdots, & 0 \\ \delta_2, & \delta_1, & 2, & \cdots, & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \delta_k, & \delta_{k-1}, & \delta_{k-2}, & \cdots, & k \\ \delta_v, & \delta_{v-1}, & \delta_{v-2}, & \cdots, & \delta_{v-k} \end{vmatrix} = 0 .$$

證：1）必要性． 如（1）式有解，命

$$R_v = t_1 x_v + t_2 x_v^2 + \cdots + t_k x_v^k,$$

則

$$\sum_{v=1}^{k} \frac{1}{x_v} R_v^2 = \sum_{i,j=1}^{k} \delta_{i+j-1} t_i t_j$$

顯然是一定正二次型．

2）充分性．（5）式一定有解的，雖然我們並不能斷定它是複數抑是實數．把 $x_1, \cdots, x_k$ 做根作一多項式、如此作出的 k 次多項式是有實係數的． 所以，如果 $x_1, \cdots, x_k$ 中有複數出現，一定是一對對的共軛複數． $x_1, \cdots, x_k$ 各不相同，且無一是零． 如若不然，$R_v = 0$ $(1 \leqslant v \leqslant k)$ 有一非零解 $(t_1, \cdots, t_k)$，(零解我們是指 $t_1 = 0, \cdots, t_k = 0$ 這一解)．因而 (2) 非定正型． 把根 $x_1, \cdots, x_k$ 排成

$$\begin{aligned} x_{2m-1} &= y_{2m-1} + i\, y_{2m}, \\ x_{2m} &= y_{2m-1} - i\, y_{2m}, \end{aligned} \qquad y_{2m} \neq 0, \qquad 1 \leqslant m \leqslant g$$

及

$$x'_\nu = y_\nu \qquad 2g < \nu \leqslant k,$$

此處 y 是實數．寫

$$\begin{aligned} R_{2m-1}/x_{2m-1} &= P_{2m-1} + iP_{2m}, \\ R_{2m}\ /x_{2m} &= P_{2m-1} - iP_{2m}, \end{aligned} \qquad 1 \leqslant m \leqslant g,$$

此處 P_ν $(1 \leqslant \nu \leqslant 2g)$ 是 $t_1, \cdots, t_k$ 的實係數線性式．解方程組

$$\begin{aligned} P_\nu &= 0, & 3 \leqslant \nu \leqslant 2g, \\ R_\nu &= 0, & 2g < \nu \leqslant k. \end{aligned}$$

及

$$y_1 P_1 = \left(-y_2 + \sqrt{y_1^2 + y_2^2}\right) P_2.$$

這是 $k-1$ 個實係數的線性方程,有 k 個變數 $t_1, \cdots, t_k$．顯然有一不同於零解的解答 $t_1, \cdots, t_k$．對這一解,我們有

$$\sum_{\nu=1}^{k} \frac{1}{x_\nu} \cdot R_\nu^2 = \sum_{\nu=1}^{k} x_\nu \left(\frac{R_\nu}{x_\nu}\right)^2 = x_1 \left(\frac{R_1}{x_1}\right)^2 + x_2 \left(\frac{R_2}{x_2}\right)^2 =$$

$$= 2y_1 (P_1^2 - P_2^2) + 4y_2 P_1 P_2 = 0.$$

這和 (2) 是定正型的假設相違背．所以 $x_1, \cdots, x_k$ 都是實數．由

$$\sum_{\nu=1}^{k} \frac{1}{x_\nu} R_\nu^2$$

的形式,立刻可以看出：如果上式是定正型,則 x_ν 都是正數．

附記：由於連續性,引理 10·7 可以作如下的修改而仍然眞實：一方面取消條件 $x_i \neq x_j$,另一方面把定正性改爲半定正性．更推廣些,有

引理 11·2. 命 $s \geqslant k$．方程組

$$x_1^h + \cdots x_s^h = \delta_h, \qquad 1 \leqslant h \leqslant k,$$

有正實數解的必要且充分條件是：有 $s-k$ 個正數 $\delta_{k+1}, \cdots, \delta_s$ 存在使

$$\sum_{i,j=1}^{s} \delta_{i+j-1} t_i t_j$$

是一半定正型，而 δ_v $(v > s)$ 是由次之關係巡迴地定義出來的：

$$\begin{vmatrix} \delta_1, & 1, & 0, & \cdots 0, \\ \delta_2, & \delta_1, & 2, & \cdots 0, \\ \cdots & \cdots & \cdots & \cdots \\ \delta_k, & \delta_{k-1}, & \delta_{k-2}, & \cdots k, \\ \delta_v, & \delta_{v-1}, & \delta_{v-2}, & \cdots \delta_{v-k} \end{vmatrix} = 0.$$

因爲和引理 10·7 的證明相同，所以略去不證.

附記：如果僅須實數解，而不限定是正數解，則

$$\sum_{i,j=1}^{n} \delta_{i+j-2} t_i t_j, \qquad \delta_0 = s,$$

的半定正性就可以保證.

引理 11·3. 如有 $k-1$ 個正數 $\delta_1, \cdots, \delta_{k-1}$ 及 $\delta_k = 1$ 適合引理 10·8 的條件，命 $N_v = [\delta_v P^v]$，則對這一組 $N_1, \cdots, N_k$ 正可解條件有了保證.

這引理的證明十分顯然. 當然我們還可以把加於 δ 的條件改變成爲加於 N 的條件.

§3. 奇異級數與相合可解條件

今用 $\sum\limits_{x,(q)}$ 代表一和，其中的變數經過一完整剩餘系，mod q. 又用 $\sum\limits_{x,(q)}'$ 代表一和，其中的變數經過一旣約剩餘系，mod q. 已有

$$\mathfrak{S}=\mathfrak{S}(N_k,\cdots,N_1)=\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}A(q_k,\cdots,q_1),$$

$$A(q_k,\cdots,q_1)=\sum_{h_1(q_1)}{}'\cdots\sum_{h_k(q_k)}{}'\ T^s e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right),$$

$$T=T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{\varphi(q_1\cdots q_k)}\sum_{x(q_1\cdots q_k)}{}'\ e\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right).$$

引理 11·4. $\mathfrak{S}$ 亦可以改寫成

$$\mathfrak{S}=\sum_{Q=1}^{\infty}\sum_{\substack{a_k=1\\(a_k,\cdots,a_1,Q)=1}}^{Q}\cdots\sum_{a_1=1}^{Q}\left(\frac{1}{\varphi(Q)}\sum_{x(Q)}{}'\ e_Q(a_kx^k+\cdots+a_1x)\right)^s e_Q(-a_kN_k-\cdots-a_1N_1).$$

證：這一引理是以下的事實的直接推理：關係

$$h_lQ/q_l=a_l,\qquad l=1,2,\cdots,k.$$

（這 Q 是 $q_1,\cdots,q_k$ 的最小公倍數），建立以下二數列的一一對應：(i) $\mathfrak{S}$ 的原定義中所展過的數列

$$q_l=1,2,3,\cdots,\quad (h_l,q_l)=1,\quad 1\leqslant h_l\leqslant q_l,\quad l=1,2,\cdots,k;$$

及 (ii) 引理中所展過的數列

$$Q=1,2,3,\cdots,\quad (a_k,\cdots,a_1,Q)=1,\quad 1\leqslant a_l\leqslant Q,\quad l=1,2,\cdots,k.$$

這一事實幾乎顯然，所以不加證明．因為

$$q_1^{-1}\cdots q_k^{-1}\sum_{x=1}^{q_1\cdots q_k}=Q^{-1}\sum_{x=1}^{Q},$$

所以得出本引理．

命 $W(m)$ 代表相合式組

$$\left.\begin{array}{l} h_1^k + \cdots + h_s^k = N_k \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ h_1 + \cdots + h_s = N_1 \end{array}\right\} \pmod m, \qquad (1)$$

$$1 \leqslant h_\nu \leqslant m, \quad (h_\nu, m) = 1, \quad 1 \leqslant \nu \leqslant s,$$

的解數．顯然可證

引理 11·5. 若 $(m_1, m_2) = 1$，則

$$W(m_1 m_2) = W(m_1) W(m_2).$$

定義.

$$A(Q) = \sum_{\substack{a_k=1 \\ (a_k,\cdots,a_1,Q)=1}}^{Q} \cdots \sum_{a_1=1}^{Q} \left(\frac{1}{\varphi(Q)} T\left(\frac{a_k}{Q}, \cdots, \frac{a_1}{Q}\right)\right)^s e_Q(-a_k N_k - \cdots - a_1 N_1)$$

及

$$\partial_p = \sum_{l=0}^{\infty} A(p^l), \qquad A(1) = 1.$$

引理 11·6.

$$\sum_{m=0}^{l} A(p^m) = p^{lk} \varphi^{-s}(p^l) W(p^l).$$

證：顯然

$$W(p^l) = \frac{1}{p^{lk}} \sum_{h_1=1}^{p^l} \cdots \sum_{h_k=1}^{p^l} \sum_{x_1=1}^{p^l}{}' \cdots \sum_{x_s=1}^{p^l}{}'$$

$$e_{p^l}\Big(h_k(x_1^k + \cdots + x_s^k - N_k) + \cdots + h_1(x_1 + \cdots + x_s - N_1)\Big) =$$

$$= \frac{1}{p^{lk}} \varphi^s(p^l) \sum_{h_1=1}^{p^l} \cdots \sum_{h_k=1}^{p^l} \left(\frac{1}{\varphi(p^l)} T\left(\frac{h_k}{p^l}, \cdots, \frac{h_1}{p^l}\right)\right)^s e_{p^l}(-h_k N_k - \cdots - h_1 N_1) =$$

$$= \frac{1}{p^{lk}} \varphi^s(p^l) \Big(\sum_{p|h_1} \cdots \sum_{p|h_k} \left(\frac{1}{\varphi(p^l)} T\left(\frac{h_k}{p^l}, \cdots, \frac{h_1}{p^l}\right)\right)^s e_{p^l}(-h_k N_k - \cdots - h_1 N_1) +$$

$$+ A(p^l)\Big)$$

$$= \frac{1}{p^{lk}} \varphi^s(p^l)\Big(\sum_{h_1=1}^{p^{l-1}} \cdots \sum_{h_k=1}^{p^{l-1}} \Big(\frac{p}{\varphi(p^l)} T\Big(\frac{h_k}{p^{l-1}}, \cdots, \frac{h_1}{p^{l-1}}\Big)\Big)^s e_{p^{l-1}}(-h_kN_k -$$

$$- \cdots - h_1N_1) + A(p^l)\Big).$$

由於 $\varphi(p^l) = p\varphi(p^{l-1})$，續行此法可得本引理.

引理 11·7. 當 $s > k^2$ 時，∂_p 收斂；且當 $s > k^2 + k$ 時，有

$$|\partial_p - 1| \leqslant 2(2k^3)^s p^{k-as}$$

及

$$\mathfrak{S} = \prod_p \partial_p .$$

證：由第一章基本引理已知

$$\left| T\Big(\frac{h_k}{p^l}, \cdots, \frac{h_1}{p^l}\Big) \right| \leqslant k^3 p^{l(1-a)} .$$

由此

$$|A(p^l)| \leqslant (p^{lk} - p^{(l-1)k}) \Big(\frac{k^3 p^{l(1-a)}}{p^{l-1}(p-1)}\Big)^s < (2k^3)^s p^{l(k-as)} .$$

所以當 $s > k^2$ 時，∂_p 絕對收斂. 又當 $s > k^2 + k$ 時，

$$|\partial_p - 1| \leqslant (2k^3)^s \sum_{l=1}^{\infty} p^{l(k-as)} \leqslant (2k^3)^s \frac{p^{k-as}}{1 - p^{k-as}} \leqslant 2(2k^3)^s p^{k-as} .$$

最後一個結論，由

$$\prod_p p^{k-as}$$

的收斂性得之.

說明：由引理 11·6 及 11·7，可知

$$\partial_p = \lim_{l \to \infty} p^{lk} \varphi^{-s}(p^l)\, W(p^l) .$$

容易看出，如果有一 l_0 使 $W(p^{l_0}) = 0$，則顯然對 $l > l_0$，$W(p^l)$ 也等於 0．所以 $\partial_p = 0$ 及 $\mathfrak{S} = 0$．具體地說：如果相合式 (1) 不可解，則我們所討論的問題就無解答．這是一十分自然的現象，也是相合可解條件命名的理由．引理 11·7 還告訴了我們另一事實：

引理 11·8. 當 $p > (2(2k^3)^s)^{\frac{1}{s-k}}$ 時，

$$\partial_p > 0,$$

即相合式 (1) 當 $m = p^l$ 時常可解．

命

$$D = \begin{vmatrix} k^{k-1}, & \cdots, & 2^{k-1}, & 1^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ k, & \cdots, & 2, & 1 \\ 1, & \cdots, & 1, & 1 \end{vmatrix} = (k-1)!\,(k-2)!\cdots 2!\,1!$$

及 $p^{\Theta} \| D$．則當 $p > k$ 時 $\Theta = 0$．命

$$p^{\Theta_\nu} \| \nu, \qquad \nu = p^{\Theta_\nu} \nu_0, \qquad \Theta_0 = \max(\Theta_1, \cdots, \Theta_k).$$

命 $W_1(p^l)$ 代表下列相合式組的解數：

$$\left.\begin{array}{c} y_1^k + \cdots + y_s^k \equiv N_k \\ \cdots\cdots\cdots\cdots \\ y_1 + \cdots + y_s \equiv N_1 \end{array}\right\} \pmod{p^l},\ p \nmid y,$$

其中

$$1 \leqslant y_\nu \leqslant p^l, \qquad 1 \leqslant \nu \leqslant k, \qquad 1 \leqslant y_\mu \leqslant p^{l-\Theta-\Theta_0}, \qquad k+1 \leqslant \mu \leqslant s$$

及

$$p^{\Theta} \| \begin{vmatrix} y_k^{k-1}, & \cdots, & y_1^{k-1} \\ \cdots & \cdots & \cdots \\ y_k, & \cdots, & y_1 \\ 1, & \cdots, & 1 \end{vmatrix}.$$

引理 11·9. 相合式組

$$\sum_{\beta=1}^{k} a_{\alpha\beta}x_\beta \equiv b_\alpha \pmod{p^l},\quad 1 \leqslant \alpha \leqslant k,$$

$$p^\lambda \| \begin{vmatrix} a_{11}, \cdots, & a_{1k} \\ \cdots\cdots\cdots\cdots & \\ a_{k1}, \cdots, & a_{kk} \end{vmatrix},$$

可解的條件是:

$$p^\lambda \mid \begin{vmatrix} b_1, a_{12}, \cdots, a_{1k} \\ \cdots\cdots\cdots\cdots \\ b_k, a_{k2}, \cdots, a_{kk} \end{vmatrix}, \cdots, p^\lambda \mid \begin{vmatrix} a_{11}, \cdots, a_{1k-1}, b_1 \\ \cdots\cdots\cdots\cdots \\ a_{k1}, \cdots, a_{kk-1}, b_k \end{vmatrix}.$$

證: 這引理可用通常的行列式的方法證明.

引理 11·10. 當 $l \geqslant 2\Theta + 2\Theta_0 + 1$, 則

$$W_1(p^{l+1}) \geqslant p^{s-k} W_1(p^l).$$

連續運用多次可得

$$W_1(p^{l+u}) \geqslant p^{u(s-k)} W_1(p^l).$$

證: 假定我們已經有了

$$\sum_{\mu=1}^{s} y_\mu^\nu \equiv N_\nu \pmod{p^l}, \tag{1}$$

$$1 \leqslant y_\lambda \leqslant p^l,\quad 1 \leqslant \lambda \leqslant k;\quad 1 \leqslant y_\tau \leqslant p^{l-\Theta-\Theta_0},\quad k+1 \leqslant \tau \leqslant s.$$

命

$$h_\mu = y_\mu + z_\mu p^{l-\Theta_0-\Theta},$$

則

$$h_\mu^\nu \equiv y_\mu^\nu + \nu y_\mu^{\nu-1} z_\mu p^{l-\Theta_0-\Theta} \pmod{p^{2(l-\Theta_0-\Theta)}},$$

$$\sum_{\mu=1}^{s} h_{\mu}^{\nu} \equiv \sum_{\mu=1}^{s} y_{\mu}^{\nu} + \nu \sum_{\mu=1}^{s} y_{\mu}^{\nu-1} z_{\mu} p^{l-\theta_0-\theta} \pmod{p^{l+1}} . \tag{2}$$

今討論相合式組

$$\sum_{\mu=1}^{s} \nu_0 y_{\mu}^{\nu-1} z_{\mu} \equiv \frac{N_{\nu} - \sum_{\mu=1}^{s} y_{\mu}^{\nu}}{p^{l-\theta_0-\theta+\theta_{\nu}}} \pmod{p^{\theta_0+\theta+1}} . \tag{3}$$

如果 (2) 及 (3) 有解,則

$$\sum_{\mu=1}^{s} h_{\mu}^{\nu} \equiv N_{\nu} \pmod{p^{l+1}} . \tag{4}$$

由於

$$p^{\theta} \parallel \begin{vmatrix} y_1^{k-1}, & \cdots, & y_k^{k-1} \\ \cdots & \cdots & \cdots \\ y_1^0, & \cdots, & y_k^0 \end{vmatrix}$$

及

$$p^{\theta} \mid p^{\theta_0+\theta-\theta_{\nu}} \mid \frac{N_{\nu} - \sum_{\mu=1}^{s} y_{\mu}^{\nu}}{p^{l-\theta_0-\theta+\theta_{\nu}}} ,$$

所以對任意的 z_{τ} $(k+1 \leqslant \tau \leqslant s)$, 相合式組 (3) 式常可解. 所以

$$W_1(p^{l+1}) \geqslant p^{s-k} W_1(p^l) .$$

證明中如無以下的補充,還不能算是完整的: 由於 $h_{\mu} \equiv y_{\mu} \pmod{p^{l-\theta_0-\theta}}$,所以

$$\begin{vmatrix} y_1^{k-1}, & \cdots, & y_k^{k-1} \\ \cdots & \cdots & \cdots \\ y_1^0, & \cdots, & y_k^0 \end{vmatrix} \equiv \begin{vmatrix} h_1^{k-1}, & \cdots, & h_k^{k-1} \\ \cdots & \cdots & \cdots \\ h_1^0, & \cdots, & h_k^0 \end{vmatrix} \pmod{p^{\theta+1}},$$

此處用了 $l > \theta_0 + 2\theta$.

引理 11·11. 設 $s > k^2 + k$，並設當 $p \leqslant (2(2k^3)^s)^{\frac{1}{as-k}}$時，

$$W_1(p^{2\theta+2\theta_0}) > 0,$$

則 $\mathfrak{S}(N_k, \cdots, N_1)$ 大於一並不依賴於 N 的常數.

證：由假定及引理 11·10 已知，當 $p \leqslant (2(2k^3)^s)^{\frac{1}{as-k}}$ 時，

$$\begin{aligned}\partial_p &= \lim_{l\to\infty} p^{lk}\varphi^{-s}(p^l)\, W(p^l) \geqslant \\ &\geqslant \lim_{l\to\infty} p^{lk}\varphi^{-s}(p^l)\, W_1(p^l) \geqslant \\ &\geqslant \lim_{l\to\infty} p^{lk}\varphi^{-s}(p^l)\, p^{(s-k)(l-2\theta-2\theta_0)}\, W_1(p^{2\theta+2\theta_0}) \geqslant \\ &\geqslant \lim_{l\to\infty} \frac{p^{-l(s-k)}}{(1-1/p)^s}\, p^{(s-k)(l-2\theta-2\theta_0)} = \\ &= p^{-(s-k)(2\theta-2\theta_0)}\left(1-\frac{1}{p}\right)^{-s} \geqslant c_1,\end{aligned}$$

這 c_1（及今後 c_2, c_3）與 N 無關，且 > 0.

命 $s = k^2 + k + \delta$，則

$$\partial_p > 1 - 2(2k^3)^s p^{-1-\delta a}.$$

當 p 適合 $(2(2k^3)^s)^{\frac{1}{as-k}} < p \leqslant (2(2k^3))^{2k/\delta}$，顯然 $\partial_p \geqslant c_2$.

又當 $p > (2(2k^3))^{2k/\delta}$，則

$$\partial_p > 1 - p^{-1-\frac{1}{2}\delta a}.$$

所以

$$\prod_{p > (2(2k^3))^{2k/\delta}} \partial_p \geqslant c_3.$$

總之，可知

$$\mathfrak{S}(N_k, \cdots, N_1) \geqslant (c_1 c_2)^{(2(2k^3))^{2k/\delta}}\, c_3.$$

引理已經證明.

今再進一步討論使

$$W_1(p^{2\theta+2\theta_0}) \geqslant 1$$

的條件.

引理 11·12. 若 $p > k$ 及 $s > (k+1)p$, 則 $W_1(p) \geqslant 1$.

證: 相合式組

$$x_1(k+1)^\nu + x_2 k^\nu + x_3(k-1)^\nu + \cdots + x_{k+1} 1^\nu \equiv N_\nu \pmod p,\ 1 \leqslant \nu \leqslant k,$$

$$x_1 + x_2 + x_3 + \cdots + x_{k+1} \equiv s \pmod p$$

常有解在 $0 < x_\nu \leqslant p$ 中. 故可取 x_{k+1} 使

$$x_1 + \cdots + x_{k+1} = s.$$

所以得出本引理.

引理 11·13. 當 $s > 2k$ 及 $p > k^{k(s-k)/(s-2k)}$ 時,相合式組

$$x_1^\nu + \cdots + x_s^\nu \equiv N_\nu \pmod p,\ p \nmid x,\ 1 \leqslant \nu \leqslant k,$$

有解.

證: 這相合式的根的組數 M 顯然等於

$$\frac{1}{p^k} \sum_{a_1=1}^{p} \cdots \sum_{a_k=1}^{p} \left(\sum_{x=1}^{p-1} e_p(a_k x^k + \cdots + a_1 x) \right)^s e_p(-(a_k N_k + \cdots + a_1 N_1)).$$

故

$$|M - p^{s-k}| \leqslant \frac{1}{p^k} \sum_{a_1=1}^{p} \cdots \sum_{a_k=1}^{p}{}^{*} \left| \sum_{x=1}^{p-1} e_p(a_k x^k + \cdots + a_1 x) \right|^s,$$

此處 * 乃表示 p 不能同時整除所有的 a. 由第一章 § 3 公式 (2) 及 (3) 得出

$$|M - p^{s-k}| \leqslant \frac{1}{p^k} (k p^{1-\alpha})^{s-2k} \sum_{a_1=1}^{p} \cdots \sum_{a_k=1}^{p} \left| \sum_{x=1}^{p-1} e_p(a_k x^k + \cdots + a_1 x) \right|^{2k} \leqslant$$

$$\leqslant \frac{1}{p^k}(kp^{1-a})^{s-2k}k!\,p^{2k} \leqslant$$

$$\leqslant k^{s-k}p^{s-k-a(s-2k)} <$$

$$< p^{s-k},$$

在條件 $p > k^{k(s-k)/(s-2k)}$ 之下. 因此得出

$$M \geqslant p^{s-1} - (p^{s-1} - 1) = 1.$$

此卽本引理.

引理 11·14. 當 $s > 3k$ 及 $p > k^{k(s-k)/(s-2k)}$ 時,則

$$W_1(p) \geqslant 1.$$

證: 由引理 11·18,當 $t > 2k$, $p > k^{k(s-k)/(s-2k)}$ 時,相合式組

$$x_1^v + \cdots + x_t^v \equiv N_v - 1^v - 2^v - \cdots - k^v, \qquad 1 \leqslant v \leqslant k,$$

常有解. 由此得出本引理.

附記: 本節所論的結果十分粗略,大有更進一步的可能.

§ 4.

引理 11·15. 命

$$(2v-1)Q \leqslant x_v \leqslant 2vQ, \qquad 1 \leqslant v \leqslant k.$$

則整數組 $x_1, \cdots, x_k$ 中,使

$$x_1^h + \cdots + x_k^h, \qquad 1 \leqslant h \leqslant k,$$

各在長 $\ll Q^{h-1}(1 \leqslant h \leqslant k)$ 的隔間中的組數 $\ll 1$.

這引理的證明如同引理 5·1 的證明,不要經過任何基本上的改變.

引理 11·16. 命 R_k 表方程組

$$\sum_{j=1}^{n}\sum_{i=1}^{k} x_{ij}^{h} = \sum_{j=1}^{n}\sum_{i=1}^{k} x_{ij}'^{h}, \quad 1 \leqslant h \leqslant k, \tag{1}$$

$$(2i-1)P^{(1-a)^{j-1}} \leqslant x_{ij}, x_{ij}' \leqslant 2iP^{(1-a)^{j-1}}, \tag{2}$$

的整數解的組數. 則

$$R_k \leqslant P^{(2k^2-\frac{1}{2}k(k+1))(1-(1-a)^n)}.$$

證: 由 (1) 及 (2) 易見

$$\sum_{i=1}^{k} x_{i1}^{h} - \sum_{i=1}^{k} x_{i1}'^{h} \ll P^{h(1-a)}, \qquad 1 \leqslant h \leqslant k.$$

對已定的 x_{i1}' $(i = 1, \cdots, k)$,

$$\sum_{i=1}^{k} x_{i1}^{k}, \sum_{i=1}^{k} x_{i1}^{k-1}, \cdots, \sum_{i=1}^{k} x_{i1}$$

各在長是

$$O(P^{k(1-a)}),\ O(P^{(k-1)(1-a)}), \cdots,\ O(P^{(1-a)}) \tag{3}$$

的隔間中. 把 (3) 的隔間組分爲

$$O\left(\frac{P^{k(1-a)}}{P^{k-1}} \quad \frac{P^{(k-1)(1-a)}}{P^{k-2}} \quad \cdots \quad \frac{P^{2(1-a)}}{P} \quad \frac{P^{1-a}}{1}\right) = O(P^{k-\frac{1}{2}(k+1)})$$

個組,而每一組是由長爲

$$O(P^{k-1}),\ O(P^{k-2}), \cdots,\ O(P),\ O(1)$$

的隔間所組成的. 由引理 11·15 (取 $Q = P$), 可知 $x_{i1}(1 \leqslant i \leqslant k)$ 的組數 $\ll P^{k-\frac{1}{2}(k+1)}$. 因此 x_{i1} 及 x_{i1}' $(i = 1, \cdots, k)$ 的組數是

$$\ll P^{2k-\frac{1}{2}(k+1)}.$$

又，對已定的 x_{ij}，x'_{ij}（$1\leqslant i\leqslant k$，$1\leqslant j\leqslant l-1$）及 x'_{il}（$1\leqslant i\leqslant k$），由（1）及（2）可知

$$\sum_{i=1}^{k} x_{il}^{k},\ \sum_{i=1}^{k} x_{il}^{k-1},\ \cdots,\ \sum_{i=1}^{k} x_{il}$$

各在長是

$$O(P^{k(1-a)^l}),\ O(P^{(k-1)(1-a)^l}),\ \cdots,\ O(P^{(1-a)^l})$$

的隔間中．由於

$$O\left(\frac{P^{k(1-a)^l}}{P^{(k-1)(1-a)^{l-2}}}\ \frac{P^{(k-1)(1-a)^l}}{P^{(k-2)(1-a)^{l-2}}}\ \cdots\ \frac{P^{(1-a)^l}}{1}\right)=O(P^{(k-\frac{1}{2}(k+1))(1-a)^{l-1}})$$

及由引理 11·15（取 $Q=P^{(1-a)^{l-1}}$）可知 x_{il}（$1\leqslant i\leqslant k$）的組數是

$$O(P^{(k-\frac{1}{2}(k+1))(1-a)^{l-1}}).$$

因此，對已定的 x_{ij}，x'_{ij}（$1\leqslant i\leqslant k$，$1\leqslant j\leqslant l-1$），$x_{il}$ 及 x'_{il} 的組數是

$$O(P^{(2k-\frac{1}{2}(k+1))(1-a)^{l-1}}).$$

所以（1）式受（2）式限制的解數

$$\ll P^{(2k-\frac{1}{2}(k+1))(1+(1-a)+\cdots+(1-a)^{\eta-1})}=$$

$$=P^{(2k^2-\frac{1}{2}k(k+1))(1-(1-a)^{\eta})}.$$

§ 5.

命

$$S_0=\sum_{n\leqslant 2P} e(\alpha_k n^k+\cdots+\alpha_1),$$

$$S_{ij}(\alpha_k,\cdots,\alpha_1)=\sum_{(2i-1)P^{(1-a)^{j-1}}\leqslant n\leqslant 2iP^{(1-a)^{j-1}}} e(\alpha_k n^k+\cdots+\alpha_1 n),$$

此處 $1\leqslant i\leqslant k$，$1\leqslant j\leqslant \eta$．

引 理 11·17. 命 $t = k^2 + 1$ 及

$$n = \left[\frac{\log(60\,k^3 \log k)}{-\log(1-a)}\right] + 1,$$

則

$$\int_0^1 \cdots \int_0^1 |S_0|^{2t} \prod_{j=1}^{n} \prod_{i=1}^{k} |S_{ij}|^2 \, d\alpha_k \cdots d\alpha_1 \ll P^{2t+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}.$$

證：如定理 16 證明中的方法來分割積分的範圍．由於$t \geqslant k^2 + 1$，所以

$$\sum_{\mathfrak{M}} \int \underset{\mathfrak{M}}{\cdots} \int |S_0|^{2t} \, d\alpha_k \cdots d\alpha_1 \ll P^{2t-\frac{1}{2}k(k+1)}.$$

(一如定理 16 中之所爲)．因此

$$\sum_{\mathfrak{M}} \int \underset{\mathfrak{M}}{\cdots} \int |S_0|^{2t} \left| \prod_{j=1}^{n} \prod_{i=1}^{k} S_{ij} \right|^2 d\alpha_k \cdots d\alpha_1 \ll$$

$$\ll \max_{a} \left| \prod_{j=1}^{n} \prod_{i=1}^{k} S_{ij} \right|^2 \times \sum_{\mathfrak{M}} \int \underset{\mathfrak{M}}{\cdots} \int |S_0|^{2t} \, d\alpha_k \cdots d\alpha_1 \ll$$

$$\ll P^{2k^2(1-(1-a)^n)} \cdot P^{2t-\frac{1}{2}k(k+1)} = P^{2t+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}.$$

又由第十章 §3 中的 7)，已知在 E 上

$$S_0 \ll P^{1-\lambda}, \quad \lambda = \frac{1}{60\,k^3 \log k},$$

及引理 11·16，

$$\int \underset{E}{\cdots} \int |S_0|^{2t} \left| \prod_{j=1}^{n} \prod_{i=1}^{k} S_{ij} \right|^2 d\alpha_k \cdots d\alpha_1 \ll$$

$$\ll P^{2t(1-\lambda)} \int_0^1 \cdots \int_0^1 \left| \prod_{j=1}^{n} \prod_{i=1}^{k} S_{ij} \right|^2 d\alpha_k \cdots d\alpha_1 \ll$$

$$\ll P^{2t-2t\lambda+(2k^2-\frac{1}{2}k(k+1))(1-(1-a)^n)} \ll P^{2t+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)},$$

此處用了

$$\frac{1}{2}k(k+1)(1-a)^n \leqslant t(1-a)^n < 2t\lambda .$$

引理 11·17 已完全證明.

§ 6.

對應地定義

$$\mathfrak{T}_0(\alpha_k, \cdots, \alpha_1) = \sum_{p \leqslant 2P} e(\alpha_k p^k + \cdots + \alpha_1 p),$$

$$\mathfrak{T}_{ij}(\alpha_k, \cdots, \alpha_1) = \sum_{(2i-1)P^{(1-a)^{j-1}} \leqslant p \leqslant 2iP^{(1-a)^{j-1}}} e(\alpha_k p^k + \cdots + \alpha_1 p),$$

$1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant n$. 命 $t = \left[\frac{1}{2}(k^2+3)\right]$ 及

$$\Omega = \mathfrak{T}_0^{2t+1} \prod_{j=1}^{n} \prod_{i=1}^{k} \mathfrak{T}_{ij}^2 = \sum I'(N_k, \cdots, N_1) e(N_k \alpha_k + \cdots + N_1 \alpha_1),$$

此處 $I'(N_k, \cdots, N_1)$ 是下列方程組的解的組數

$$\sum_{i=1}^{k} \sum_{j=1}^{n} p_{ij}^h + \sum_{i=1}^{k} \sum_{j=1}^{n} p_{ij}'^h + \sum_{\nu=1}^{2t+1} p_\nu''^h = N_h, \quad 1 \leqslant h \leqslant k,$$

$$(2i-1)P^{(1-a)^{j-1}} \leqslant p_{ij}, p_{ij}' \leqslant 2iP^{(1-a)^{j-1}}, \ 1 \leqslant p_\nu'' \leqslant 2kP,$$

此處 $2kP = N_k^a$.

引理 11·18.

$$I'(N_k, \cdots, N_1) = \frac{b_2 P^{2t+1+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}}{L^{2t+1+2kn}} \mathfrak{S}(N_k, \cdots, N_1) \times$$

$$\times\left(1+O\left(\frac{\log L}{L}\right)\right).$$

此處

$$b_2=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left\{\left(\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx\right)^{2t+1}\times\right.$$

$$\times\prod_{\nu=1}^{k}\left(\int_{(\nu-1)a}^{\nu a} e(\gamma_k x^k+\cdots+\gamma_1 x)\,dx\right)^2\times$$

$$\left.\times\, e\left(-\frac{N_k}{(2kP)^k}\gamma_k-\cdots-\frac{N_1}{2kP}\gamma_1\right)\right\}d\gamma_k\cdots d\gamma_1 .$$

證：我們有

$$I'(N_k,\cdots,N_1)=\int_0^1\cdots\int_0^1 \mathfrak{T}_0^{2t+1}\prod_{j=1}^{n}\prod_{i=1}^{k}\mathfrak{T}_{ij}^2\, e(-N_k\alpha_k-\cdots-N_1\alpha_1)\,d\alpha_k\cdots d\alpha_1 .$$

如定理 17 的證明方法來分割積分範圍. 由引理 10·8 已知

$$\int\cdots\int_{\mathfrak{E}}\left|\mathfrak{T}_0^{2t+1}\prod_{j=1}^{n}\prod_{i=1}^{k}\mathfrak{T}_{ij}^2\right|d\alpha_k\cdots d\alpha_1\ll$$

$$\ll PL^{-\sigma_1}\int_0^1\cdots\int_0^1|\mathfrak{T}_0|^{2t}\prod_{j=1}^{n}\prod_{i=1}^{k}|\mathfrak{T}_{ij}|^2\,d\alpha_k\cdots d\alpha_1\ll$$

$$\ll PL^{-\sigma_1}\int_0^1\cdots\int_0^1|S_0|^{2t}\prod_{j=1}^{n}\prod_{i=1}^{k}|S_{ij}|^2\,d\alpha_k\cdots d\alpha_1\ll$$

$$\ll P^{2t+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}L^{-\sigma_1}.$$

一如定理 17 的證明,可證

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}}\mathfrak{T}_0^{2t+1}\prod_{i=1}^{k}\mathfrak{T}_{i1}^2\, e(-N_k\alpha_k-\cdots-N_1\alpha_1)\,d\alpha_k\cdots d\alpha_1=$$

$$=b_2\,\mathfrak{S}(N)\,P^{2t+2k+1-\frac{1}{2}k(k+1)}L^{-2t-2k-1}\left(1+O\left(\frac{\log L}{L}\right)\right),$$

此處

$$b_i = \int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left\{\left(\int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\,dx\right)^{2s+i}\times\right.$$

$$\times\prod_{\nu=1}^{k}\left(\int_{(\nu-1)/k}^{\nu/k} e(\gamma_k x^k + \cdots + \gamma_1 x)\,dx\right)^{l}\times$$

$$\left.\times\, e\left(-\frac{N_k}{(2kP)^k}\gamma_k - \cdots - \frac{N_1}{2kP}\gamma_1\right)\right\}d\gamma_k\cdots d\gamma_1.$$

再用引理 9·6 的證明中所用的方法，可以得出我們所需要的定理.

第　十　二　章

其他的結果

§ 1.

本章中將論及一些結果與問題，這些都是可以藉助於本文中所敘述的方法而獲得或解決的．這些問題依其本性可以分成下列四個範疇：

а）包含概念“幾乎一切”或“具有正密率”的問題；

б）由下列的假設而引導出來的問題：即對於任何一個預定的整數$N(>0)$，必有一整數 A 存在，使二次多項式

$$x^2 - x + A$$

當 $x = 0, 1, \cdots, N$ 時取素數值；

в）把第十章的問題推廣爲若干不同多項式之和同時表示幾個數的問題；

г）由以下的推測所引導出的推論：

方程組

$$x_1^h + \cdots + x_{\frac{1}{2}k(k+1)}^h = y_1^h + \cdots + y_{\frac{1}{2}k(k+1)}^h,\ 1 \leqslant h \leqslant k,\ 1 \leqslant x, y \leqslant P,$$

有 $\ll c_1(k) P^{\frac{1}{2}k(k+1)} (\log P)^{c_2(k)}$ 組整數解．

有些不屬於這些範疇的結果將在本章 §6 中論述之．

§ 2.

假定 $\mathfrak{M}$ 是不同的自然數所成的集合，$M(x)$ 是其中不超過 x 的元素的個數．又假定 $\mathfrak{N}$ 是集合 $\mathfrak{M}$ 的一個分集合，而 $N(x)$ 是 $\mathfrak{N}$ 中不超過 x 的元素的個數．如果

$$\lim_{x\to\infty}\frac{N(x)}{M(x)}=1,$$

則我們說：$\mathfrak{N}$ 幾乎包含了 $\mathfrak{M}$ 的所有的元素．特別是，如果 $\mathfrak{M}$ 是由所有的 $\equiv l \pmod q$ 的正整數所組成的，我們就簡單地說：$\mathfrak{N}$ 幾乎包含了一切 $\equiv l \pmod q$ 的整數．

又如果

$$\varliminf_{x\to\infty}\frac{M(x)}{x}\geqslant\alpha>0,$$

則我們說：$\mathfrak{M}$ 具有正的漸近密率．

設 $h(k)$ 表示滿足下列條件的最小正整數 s，即凡可表示成 s 個素數 k 次方的和的形狀的整數所成的集合幾乎包含一切 $\equiv s \pmod K$ 的正整數．這 K 已在第八章中定義．我們能夠證明

$h(1)=2$，$h(2)=3$，$h(3)\leqslant5$，$h(4)\leqslant8$，$h(5)\leqslant13$，$h(6)\leqslant20$，$h(7)\leqslant28$

及

$$h(k)\leqslant k+m+4,$$

這裏 m 具有第九章 §1 的意義．

以 $f_\nu(x)$ 代表 s_0 個 k 次整值多項式，而 s_0 的定義是

k	1	2	3	4	5	6	7	$\geqslant 8$
s_0	2	3	5	8	13	20	28	$k+m+4$

則能表成

$$f_1(p_1)+\cdots+f_s(p_s)\qquad\qquad(p\text{：素數})$$

形式的整數的集合有正的漸近密率．

§3. 一個假設的陳述

對任意預給的整數 $N(>0)$，必有一整數 A 存在使

$$x^2-x+A$$

當 $x=0, 1, \cdots, N$ 時表示素數. 以下的數據支持了這一假設的真確性：當 $x=0, 1, \cdots, 40$ 時

$$x^2-x+41$$

代表素數. 又

$$x^2-x+19421,\quad x^2-x+27941,\quad x^2-x+72491$$

都代表豐富的素數（最後一個由 $x=0$ 到 $x=11000$ 都代表素數）*.

換一種說明的方法：有 $N+1$ 個方程，$N+2$ 個素數未知數 $p_m(0\leqslant m\leqslant N)$ 及 A 使

$$m^2-m+A=p_m,\quad 0\leqslant m\leqslant N,$$

可解. 消去未知數 A，則得

$$m^2-m=p_m-p_0,\quad 1\leqslant m\leqslant N,$$

即得一方程組其中有 N 個方程及 $N+1$ 個素數未知數. 把這一問題提高到更一般性：就是求解一組 N 個聯立方程其中有 $N+1$ 個素數未知數的問題：

$$\sum_{j=1}^{N+1} a_{ij}\, p_j = b_i,\quad 1\leqslant i\leqslant N. \tag{1}$$

當然要這問題有解必需要有"正可解條件"和"相合可解條件"，但在今天這一問題的解答還在數學家的能力之外，而我們所可能為力者在證明：對幾乎所有的適合相合可解條件的 b，(1) 式可解.

---

* Beeger, N. G. W. H., Report on some calculations of prime numbers, *Nieuw. Arch. Wiskde*, **20** (1939), 40–50.

但方程組

$$\sum_{j=i}^{2N+1} a_{ij} p_j = b_i, \quad 1 \leqslant i \leqslant N,$$

在正可解及相合可解條件下對所有的充分大的 b 是可解的.

最後舉出本問題中所包有的若干有趣的特例:

I) 古特拔黑問題: 方程

$$p_1 + p_2 = 2n$$

當 $n > 1$ 時可解. (此卽以上一般性的問題 $N = 1$ 時的特例).

II) 孿生素數問題: 方程

$$p_1 - p_2 = 2$$

有無窮個解.

III) 三生素數問題: 方程組

$$p_1 - p_2 = 2, \quad p_2 - p_4 = 4$$

有無窮個解. (或

$$p_1 - p_2 = 4, \quad p_2 - p_4 = 2$$

有無窮個解).

§4. 第十及十一章的方法用到更普遍的問題

命 $\{f_{i1}(x), \cdots, f_{is}(x)\}$ $(1 \leqslant i \leqslant k)$ 表 k 組, 每一組有 s 個整値多項式. 現在的問題是解方程組

$$f_{11}(p_1) + \cdots + f_{1s}(p_s) = N_1,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_{k1}(p_1) + \cdots + f_{ks}(p_s) = N_k.$$

這一類方程的解答並不太難, 如果我們假定 f 的次數是受囿的, 且 s 是相當大的話. 一般說來, 第十及第十一章的方法可用, 但須引進以下的不等式:

$$\int\cdots\int|g_1\cdots g_s|\,d\alpha_1\cdots d\alpha_k\leqslant\left(\prod_{\nu=1}^{s}\int\cdots\int|g_\nu|^s\,d\alpha_1\cdots d\alpha_k\right)^{1/s}.$$

§5. 一假設的敘述

假設：方程組

$$x_1^h+\cdots+x_{\frac{1}{2}k(k+1)}^h=y_1^h+\cdots+y_{\frac{1}{2}k(k+1)}^h,\quad 1\leqslant h\leqslant k,\quad 1\leqslant x,y\leqslant P,$$

的整數解的組數 $\leqslant c_1(k)\ P^{\frac{1}{2}k(k+1)}\ (\log P)^{c_2(k)}$.

這一假設的眞實性，當 $k=1$ 時，十分顯然．當 $k=2$ 時，已在第四章中證明了（定理 B_2'）．當 $k\geqslant 3$ 時，這是一留待解決的問題．如果能證明此點，則本書中一切的定理都可以改善．例如：解數的漸近式將當 $s>\frac{1}{2}k(k+1)$ 時眞實．這一假設的證實在解析數論中還有其他的很多的應用．

§ 6.

本節中再敘述一些其他的結果：

I) 所有的充分大的整數可以表成一個素數及 s 個素數的 k 次方的和，如果 $s\geqslant s_0\sim 2k\log k$.

II) 所有的充分大的整數可以表成一個素數及 s 個整數的 k 次方之和，如果 $s\geqslant s_0\sim\frac{3}{2}k\log k$.

III) 所有的充分大的整數可以表成 s 個不多於兩個素因子的整數的 k 乘方的和，如果 $s\geqslant s_0\sim 3k\log k$.

關於 II) 及 III) 的證明方法必須採用維諾格拉陀夫的另一創造性的方法，見 Виноградов, Метод тригонометрических сумм в теории чисел, *Труды Матем. института им. В. А. Стеклова*, т. 23, стр. 1—109，特別是其中的第四章．

$$\int\cdots\int|g_1\cdots g_s|\,d\alpha_1\cdots d\alpha_k\leqslant\left(\prod_{\nu=1}^{s}\int\cdots\int|g_\nu|^s\,d\alpha_1\cdots d\alpha_k\right)^{1/s}.$$

§5. 一假設的敘述

假設：方程組

$$x_1^h+\cdots+x_{\frac{1}{2}k(k+1)}^h=y_1^h+\cdots+y_{\frac{1}{2}k(k+1)}^h,\quad 1\leqslant h\leqslant k,\quad 1\leqslant x,y\leqslant P,$$

的整數解的組數 $\leqslant c_1(k)\ P^{\frac{1}{2}k(k+1)}\ (\log P)^{c_2(k)}$.

這一假設的眞實性，當 $k=1$ 時，十分顯然．當 $k=2$ 時，已在第四章中證明了（定理 B_2'）．當 $k\geqslant 3$ 時，這是一留待解決的問題．如果能證明此點，則本書中一切的定理都可以改善．例如：解數的漸近式將當 $s>\frac{1}{2}k(k+1)$ 時眞實．這一假設的證實在解析數論中還有其他的很多的應用．

§ 6.

本節中再敘述一些其他的結果：

I） 所有的充分大的整數可以表成一個素數及 s 個素數的 k 次方的和，如果 $s\geqslant s_0\sim 2k\log k$．

II） 所有的充分大的整數可以表成一個素數及 s 個整數的 k 次方之和，如果 $s\geqslant s_0\sim\frac{3}{2}k\log k$．

III） 所有的充分大的整數可以表成 s 個不多於兩個素因子的整數的 k 乘方的和，如果 $s\geqslant s_0\sim 3k\log k$．

關於 II） 及 III） 的證明方法必須採用維諾格拉陀夫的另一創造性的方法，見 Виноградов, Метод тригонометрических сумм в теорий чисел, *Труды Матем. института им. В. А. Стеклова*, т. 23, стр. 1—109, 特別是其中的第四章．